資　料

米国のシステム監査／セキュリティ

昭和57年 8 月

JIPDEC

財団法人　日本情報処理開発協会

この資料は，日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて昭和57年度に実施した「わが国の情報処理に関する動向調査」の成果をとりまとめたものであります。

目　　次

Ⅰ. トーシュ・ロス会計事務所

1. 会社概要

トーシュ・ロス会計事務所は，米国8大会計事務所の一つに数えられ，オーディタ6,000名を擁する会計事務所である。またわが国では，等松青木監査法人がパートナーになっている。システム監査に関しては，当社はＴＲＡＰ（Touche Ross Audit Process）と称する独自の監査技法を開発しており，また汎用監査支援ソフトウェア＂STRATA＂を開発している会計事務所である。

2. システム監査への取組

(1) 米国におけるシステム監査は，1973年にイクイティ・ファンディングの20億ドルに上る架空保険証書を発行したコンピュータ犯罪が発覚するまでは特に顕著な動きはなかった。

また，1974年12月8日に米国公認会計士協会が監査基準書（SAS）第3号を制定公表した時期を前後して，システム監査の問題が一段と活発になった。

トーシュ・ロスもこの時期に，比較的早い段階で監査技法としてＴＲＡＰを開発し，監査支援プログラム＂STRATA＂を使ってシステム監査を実施している。

3. AICPA監査基準書（SAS）第3号

従来のSAS第1号基準書を基に，コンピュータ・システムの与える影響を加味して作成されたものである。これには，全般管理と適用業務別管理についての監査基準が規定されている。

(1) 全般管理

(a) EDP作業の組織と運営のプラン

(b) システム，プログラムの開発・変更に関する文書作成，テストおよび承認の手続。

(c) ハードウェア・コントロール。

(d) 装置およびデータ・ファイルのアクセスに関する管理。

(e) EDP作業全般の手続的な管理。

(2) 適用業務別管理

a) インプット・コントロール

b) プロセシング・コントロール

c) アウトプット・コントロール

この規定は，現在でも米国でシステム監査上最低限充足すべき重要な基準となっている。トーシュ・ロスのシステム監査も，当然このＳＡＳ第３号に準拠して行なわれている。

なお当社の監査は，会計監査が本来の目的であるから，システム監査は会計監査に関連する範囲に限られている。

4. システム監査の二つの側面

システム監査には２つの段階がある。会計記録の適正性の程度を確かめるため，EDPシステムの内部統制の信頼性をレビューする段階と，取引記録のデータ処理の有効性と妥当性を検討するため，具体的にシステムのコントロールをテストする段階とがある。

前者はシステム仕様書，フローチャート，プログラムのソースコードなど，各種資料を点検レビューするものであり，後者は実際取引におけるデータの発生から最終にいたるまでのコンピュータのデータ処理上のコントロールをテストするものである。

この際，監査手段としては，コンピュータの環境周辺を監査するコンピュータ周辺監査（Auditing Around the Computer）と，コンピュータ処理過程監査（Auditing Through the Computer）の２つの方法がある。監査の完全性を

期するためには，両者を併用して監査を実施すべきであるが，コンピュータ処理自体の監査には非常に時間と経費を要するので，トーシュ・ロスにおいてはコンピュータ周辺監査が殆んどで，コンピュータ処理過程監査はあまり実施されていないのが現状である。

5. コントロールのテスト

当社が実施しているコンピュータ・システムのコントロールのテストは，次の様な内容である。

(a) データ処理上のコントロール

- パリティ・チェック
- リミット・チェック
- エディット・チェック

(b) 会計上のコントロール

- 会計証憑のチェック（Voucher Test）

(c) セキュリティ・コントロール

- 人の出入および室の施錠チェック
- 防災（火災，防水など）チェック

これらコントロール項目の中には，完全にテストすることが困難なものがある。例えば，大システムのデータ処理上のコントロール，およびＯＳに関するコントロールなどである。とくに，ＯＳの機能を監査することは非常に困難である。

6. 会計コントロールのテスト

トーシュ・ロスでは，サイクル・アプローチ法を採用している。すなわち，コンピュータ化された処理を特別視するのではなく，取引の最初から最後まで一貫した見方でコントロールをテストするアプローチをとっている。その際，トーシュ・ロスでは，サイクルを次の５サイクルに分けて考えている。

① Accounting Receivable

② Accounting Payable

③ Inventory Control

④ Payroll

⑤ Posting & Summarization

この5サイクルの中では5番目のPosting & Summarizationが会計監査上最重要である。5サイクルを通じての基本的監査の考え方は，記録と証憑の照合，すなわちバーチャー・テスト（Voucher Test）の考え方が基本である。

トーシュ・ロスでは，会計コントロールのテストの基準についてTRAP手法についてのマニュアルTRACE(Touche Ross Accounting Control Evaluation Program）に詳細な規定がある。内容としては，各サイクルの内部コントロールと監査目的（対象）に対応して

(a) 内部コントロールのキーポイント

(b) 準拠性のテスト（Compliance Tests）の仕方

(c) 実証性テスト（Substantive Tests）の仕方

が記述されている。

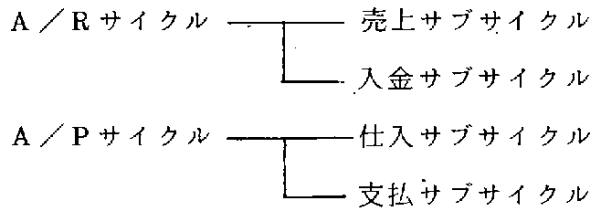
なお準拠性テストおよび実証性テストの意味は，コントロールのテストの内容である。準拠性テストは，定められたコントロールあるいは基準が遵守されているかどうかをテストすることである。実証性テストは，取引の会計処理の正当性に関して証拠を収集して，処理あるいは計算の妥当性を立証するテストである。

もとより，準拠性テストよりも実証性テストの方が確実なテストであるが，時間と経費がかかるので，トーシュ・ロスでも実際問題として準拠性テストのみで監査をとどめるケースが多いとのことである。

7. 会計コントロール・テストの具体例

A／R（売掛）サイクルとA／P（買掛）サイクルについては，次のようになる。

まず，A／RサイクルおよびA／Pサイクルは，それぞれ2つのサブサイクルに分かれる。



そして，それぞれのサイクルで業務上必要なコントロールとして，次のような証憑チェックが行なわれる。

① A／R売上サブサイクル

顧客注文書と社内受注書および送品書の金額数量などを照合し，請求書を発行し，売掛金ファイルに計上する。

② A／R入金サブサイクル

顧客よりの入金金額と売掛金ファイルを照合し，入金処理する。

③ A／P仕入サブサイクル

発注書と納品書および仕入先よりの請求書と金額・数量など照合し，買掛金ファイルに計上する。

④ A／P支払サブサイクル

買掛金ファイルと仕入先マスターを照合し，正当な支払分であれば支払伝票を発行し支払う。

それぞれのサイクルで会計管理，業務管理の面より重要なことは取引証憑の相互のマッチング（Voucher Test）である。そして，それは日常業務で，人手あるいはコンピュータで照合が行なわれている。コンピュータ監査でのコントロールのテストも，この取引証憑の相互照合に最重要なポイントが置かれる。そして会計監査としてよく行なわれる方法は，取引データをサンプリングし原始伝票とコンピュータ・アウトプット・データを人手で照合する仕方であるが，これはどちらかと言えばコンピュータ周辺監査に属するもので，監査の完璧は期し難い。とくに取引データが多い場合，業務処理が殆んどコンピュータで処理される場合，および原始データ自体がコンピュータ化されているような場合（例えば顧客の注

文書がM／Tやディスケットなどである場合）などでは，コンピュータ周辺監査の方法および準拠性テストの方法では殆んど監査の役には立たない。監査の精度を高めるためには，コンピュータ・プログラムを直接読んでチェックしたり，監査人が自ら照合プログラムを作って基本ファイル相互のマッチングをしたり，あるいは業務プログラムと同様のプログラムを別に作成して，それで処理した結果と本番データの処理結果とを照合してシステムの正当性を監査するなど，プログラムを利用したいわばスルー・ザ・コンピュータの監査手法の採用が必要になってくる。このような監査手法は時間と経費がかかり，また技術的にも困難であるが，監査の完全を期すためには実施せざるを得ないであろう。なぜなら，専門プログラマは，矛盾する機能（ Incompatible Function ）を持ち得てコンピュータ犯罪を行ない得る可能性があるからである。すなわち，プログラマは，不正なデータを創造すること（ Create Error ）もできるし，また，不正データを強制的に突合させる正当なデータとして扱う（ Cover up ）こともできるからである。そして，このような不正は，コンピュータ周辺監査やコントロールの準拠性テストでは発覚することは困難である。

8. システム監査のチェックポイント

トーシュ・ロスのシステム監査の目的ないしチェックポイントを箇条書にすれば次の通りである。

(a) Validity　取引の正当性，合法性，実在性のチェック

(b) Authorization　マネジメントにより認証されているかどうかのチェック

(c) Recoding　正当に記録されたか，実際の取引情報であるか，ソース・ドキュメントの有無などのチェック

(d) Accuracy　計算，処理の正確性のチェック

(e) Classification　取引の勘定科目の正当性のチェック

(f) Cut-off　正当な期間内の処理（タイミング）がどうかのチェック

(g) Posting & Summarization

総勘定之帳への仕訳記帳の妥当性のチェック

この点に関連して，取引情報はあくまでソース・ドキュメントと照合して始めて会計上の取引となり，また会計仕訳が行なわれない限り総勘定元帳に計上されないということがとくに強調された。

9. 会計監査におけるマイコンの利用

最近，会計監査にマイクロコンピュータを利用する方法がトーシュ・ロスではとられている。これは，監査人が必要とする会計処理をマイクロコンピュータで処理し，その結果を要約した形式でＣＲＴディスプレイまたはプリンタに出力し，会計監査の効率化を計ることを意図したものである。

当日，実際にデモンストレーションで紹介されたものは，

① 貸借対照表の計数をタテに科目，ヨコに期の計数をマトリクスの形で出力する。

② 貸借対照表・損益計算書を一括して出力する。

③ 出力画面を分割編集して必要項目を重点的に出力する。

④ ある勘定科目の計数が変更された場合，それに関連する科目の計数を再計算し，更新後の総勘定元帳を出力する。

などに利用することができることが示された。

ハードウェアの形式がOSBORNE−1で，小型のポータブル型マイクロコンピュータであることと価格が安い点に特徴がある。またバッテリーによる使用も可能であり，米国航空局より飛行機の機内での使用も認定済である。

トーシュ・ロスに設置のOSBORNE−1の構成は次の通りである。

メイン・メモリー　　64KB

標準キーボード（テン・キー）

デイスケット２ドライブ

小型ディスプレイ

ＯＳはＣＰＭ

価格は 1795 ドル（約 45 万円）

OSBORNE－1の機能としては，他にMODEMにも接続でき，OSとしてMPMを使用すれば遠隔地のコンピュータと連動し，他社の会計情報をオンラインで検索することができる。また，OSとしてCPNETを使えば，OSBORNE同志のネットワーク使用が可能である。さらに，ビデオテープによるドキュメントの画像情報をカセットテープを媒体として処理することもできる。

およそ会計監査には，証拠として膨大なハードコピーの収集が必要であるが，このOSBORNEのようなマイクロコンピュータを利用すればその必要がなくなり，いわばペーパーレス・オーディットができることになる。

10. 質疑応答

(1) Q：トーシュ・ロスには何人のシステム監査人がいるのか。

A：コンピュータ専門の監査人は小数であるが，社内にシステム監査教育コースがあり，一般監査人の殆んどがコンピュータ監査の実務をマスターし，実務を担当している。

(2) Q：会計事務所における会計士は職業法に認定されているが，コンピュータ技術者はどういう立場にあるのか。

A：社内では，コンピュータ技術者にも相当の権限と資格を与えられている。またコンピュータ技術者は，一般監査人にシステム監査の教育指導に当っている。

コンピュータ技術者にも会計士（CPA）と同じ様な資格を持っている者が社内にいる。

○コンピュータ技術者の資格

（名　　称）	（認定機関）
CISA(Certified Information System Auditor)	EDP Auditor Association
CDP(Certificate in Data	I.C.C.P(Institute for

Processing) Certification of Conputer

CCP(Certificate in Computer Professionals)

Programming)

但し，CISA，CDP，CCPの資格は大学卒程度で実務経験5年以上を必要条件とする。

(3) Q：イクイティ・ファンディング事件などの場合の監査人の責任について，およびこの事件後ＳＡＳ第3号の内容に変更があったか。

A：イクイティの場合は，責任者2名のうち1名は入獄させられたとのこと。またこの事件の関連ではＳＡＳ第3号の内容には変更があったとは聞いていない。

監査人の犯罪構成については，米国証券取引委員会の法令第3334で十分な証拠なしに監査した場合最長5年の刑の規定がある。なお，監査人の責任・犯罪などに関しては次の参考文献がある。

1) Abraham J. Briloff：Unaccountable Accounting：Prentice−Hall

2) Abraham J. Briloff：More Debit Than Credit：Prentice−Hall

(4) Q：海外不正防止法（FCPA=Foreign Corrupt Practice Act）によって監査内容が変り，プログラム等を変更しなければならなかった。

A：プログラムなどの書き換えについては聞いていない。今後いろいろ影響があると思うが，現在までではシステム監査人を必要とするようになった。

(5) Q：米国における企業の外部監査人（会計士）選定のやり方について。

A：(a)監査人のサービス面，(b)監査費用，(c)人脈などいろいろな要因で監査人が定められる。基本的には日本の場合と大差はない。

(6) Q：米国でシステム監査手法として，監査モジュールの組込，ＩＴＦ法（ミニ・カンパニー法）などの使用例は多いか。

A：殆んど使用例を聞いていない。ただ監査モジュールの組込についてはチェース・マンハッタン銀行で採用しているということである。コンピュータ・ソフト面での監査上の手法として多いのは，主に監査データを抽出するための監査支援プログラムの利用である。

例　AUDIMATE・STRATAなど

(7) Q：システム監査で利用できるIBMのSMFのようなシステム評価系のソフトウェアは何か。

A：ブール・アンド・バベッジ社（Boole & Babbage）の次の2つを知っている。

PPE(Problem Program Evaluation)

CUE(Chanel Utilization Evaluation)

11. まとめ

トーシュ・ロス会計事務所のシステム監査は，会計に関連ある範囲で行なわれ，コンピュータ周辺監査が主体で，システム・コントロールのテストも準拠性のテストが中心である。スルー・ザ・コンピュータによる監査ならびにコントロールの実証性のテストなどは，必要かつ望ましいとされながらも，時間と経費の許す範囲内で実施されているのが実情である。しかし，当社の一般監査人の殆んどが当社独自のTRAP手法によりシステム監査の実務を担当しているということは，システム監査が当社および米国会社に極めて普及定着していることを示めすものであろう。

Ⅱ. I B M

1. 会社概要

IBM社の，本社，米州／極東事業部，欧州／中東／アフリカ事業部などがニューヨークのマウント・プレザント地区にあり，この他，ワトソン研究所など数多くの施設が，この付近150キロの範囲にある。この地域の従業員は約35,000人であり，これは全世界のIBM従業員の10％にあたる。

1981年の総売上は290億ドルで，前年比11％の増加であった。但しこれは為替の変動による影響が大きく，前年と同じレートで換算すると19％の増加になる。

内訳は米国52，その他が48％で，その他のうち1／3が中南米・カナダ・極東，2／3が欧州・中東・アフリカである。

事業別にいえば83％がコンピュータ関係（ハード，ソフト，SE，CEサービス），14％が事務機器（コピー，タイプライタ等），3％が米国政府や軍関係である。

現在7,000種の製品群があり，年間16億ドルの研究費（売上の5～6％）を投資している。この他に情報処理のため社内で18億ドルのコンピュータ費用が発生しており，当社の最大の顧客はかつてはGM社であったが，現在ではIBM社自身が最大の顧客である。

昨年のフォーチュン誌の調査では，IBM社は売上高で世界9位（8位までの会社は石油関係6社およびGMとフォード），利益ではエクソンについで2位である。

事業所は，米州／極東に45か国（従業員4万5千人），欧州／中東／アフリカ80か国（10万4千人），米国（20万6千人）を含めて126か国，従業員は35万5千人である。

各国の子会社がそれぞれプロフィット・センターであるが，製品の開発は米国

本社の管理下にあり，米国，欧州，日本（藤沢）の3か所で行なっている。

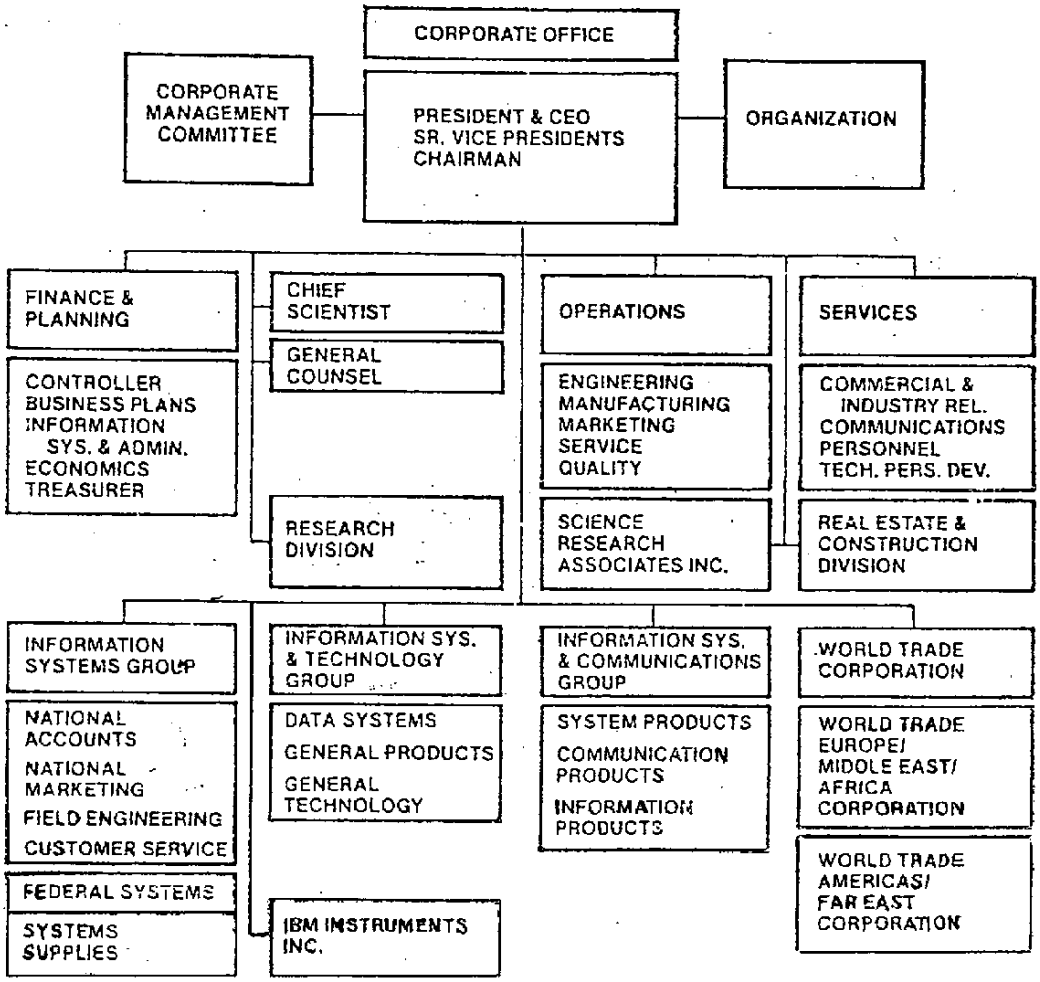


図1　ＩＢＭの組織図

2. 適用業務システムの統制と可監査性

最初にコンピュータが開発されて以来，長い間ユーザはコンピュータの情報システムに非常に信頼感を持って仕事を進めて来た。それが，1973年のイクイティ・ファンディング事件が起きて，組織の見直しが必要であることを痛切に感じた。そのことを契機としてＩＢＭでも監査業務が強化された。もう一つの大きな出来事として，1977年に海外不正防止法が制定されたことも要因となって，システムの統制と監査がさらに重要視されるようになった。

この他にも，システムに欠陥はつきものであること，誤りや犯罪を防止する完全な方法はないということ等も含めて，これら４つの理由から内部監査が推進されている。

内部監査の目的は，ＩＢＭ社内のデータ処理環境における内部統制組織の優秀さを保証するためのものであり，そのためには，①情報システム，経理，システムの所有者（オーナー）と使用者（ユーザ）の各部門に適切な人材を配置し，教育等により知識を高めること，②それに適合する規則や手法を開発して行くことが必要である。

(1) 各機能に対する責任の所在

具体的な方法としては，まずコンピュータを使うオーナーに対して，その人を認識し，その人でなければ使えないという責任を与えることにより，それ以外の人がシステムに入り込まないようにすることが重要である。

次の表は，各機能に対する責任の所在を示したものである。

（機　　能）	（責　　任）
① システムの所有者を指定する	最高機能執行者
② 業務をオーソライズする	所有者
③ 特別の機能の管理	所有者
④ 機能管理の手段	所有者と情報システム
⑤ 情報システム管理の手段の特定	情報システム
⑥ 総合管理パッケージの承認	所有者と情報システム
⑦ 必要なプログラムの検証	管理者

情報システム開発の過程は，自動車が市場に出るまでの過程と対比するとわかりやすい。

（自　動　車）	（業務システム）
市場分析	ユーザの要求の分析
会計的な分析	業務の検討
車のデザイン	システムのデザイン

機　能	機　能
効　率	効　率
統制（ブレーキ，ライト等）	可監査性
路上テスト	システムテスト
検　査	検証点検
発　売	導　入
修　繕	維　持
管　理	環境管理
	作業管理
	手順管理
	界面管理

(2)　監査部門からの指示

監査を実施するに当って，監査部門から情報システムおよびユーザ部門に対して，さまざまの指示を行なう。指示の内容は次のようなものである。

①　現在の業務システムの持続状況

②　検索および監査要求に対する記録保持

③　すべての上流システムからの流れの検証

④　外部の管理が適切であることの保証

⑤　実行に当っての危険性の確認

⑥　実行管理および可監査性の教育

⑦　実施状況の実行管理点検

このような指示書を作り，可監査性を組織の中に組込んだあとは，一過性のものでなく，持続して実施されるよう監視することが必要である。

開発された業務プログラムが実行される前に，実行すべきか否かの検定点検が行なわれる。検定点検に当っては次の点に注意しなければならない。

①　検定点検とは何か

②　どの適用業務システムについて実施するのか

③ いつ実施するのか

④ 誰の責任で実施するのか

⑤ 誰が実施するのか

⑥ どのように実施するのか

⑦ どういう効果があるのか

監査の実行には，責任とタイミングとチームが重要な要素である。ＩＢＭでは次の４人が１組となってチームを作る。

① 情報システムから１人

② 会計の業務管理から１人

③ 適用業務の熟練者から１人

④ 開発関係から１人

この４番目の人は，他の３人をサポートする役割を果す。

(3) 監査プログラムの作成

監査の方法としては，まずこの４人が集まって監査プログラムを作る。ＩＢＭでは分厚い手引書があって，どのような分野の適用業務についても，容易に監査プログラムが作れるようになっており，殆どがコンピュータで処理できるようになっている。それを使って，実際の適用業務に関する監査プログラムを作る。

出来上ったプログラムは，責任者がチェックして，管理者に渡される。管理者は次の３つの観点から，そのプログラムが実用に適しているか否かを判断する。

① プログラムが完全に必要を満たしているか。

② もっと改善する必要がないか

③ 改善すべき点は改善されているか

このような監査プログラムを開発して２年になり，その間，プログラムが管理者に理解されなかったり，使いにくかったり，さまざまな問題があったが，これらを克服しつつ現在に至っている。

監査プログラムの開発手順は次の8段階から成る。

① 概括的なルールを作る

② ルールに基づいて詳細な指示を決める

③ 指示の中で改善する部分があれば改善する

④ 一般的に使用できるような手引書として完全な形にする

⑤ 管理者が使い易さを判断する

⑥ 管理者が実際に使って見て，業務間の関連性を点検する

⑦ 管理者が各業務の担当者の相談にのる

⑧ 会社の部門間，および経営者との連絡をよくする

（質問） 監査プログラムを使って，この2年間にどのような業務の監査をして来たか。

（答） ＩＢＭ社内において，監査すべきものはすべてと言える。例えば，給与，棚卸資産，財務，営業，市場管理，管理情報システム等である。

(4) 統制の原則

監査プログラムの作成に関して，統制の原則として次の10項目を考慮しなければならない。

① 責任の分割

② できるだけ簡潔なプログラムであること

③ 適用業務のすべての領域に行きわたっているか

④ プログラムがどの範囲に使われるか

⑤ 論理的に正しいプログラムであるか

⑥ 誤りや問題を途中で示すようになっているか

⑦ 費用対効果のバランスが考慮されているか

⑧ 過度な統制になっていないか

⑨ 問題や過剰統制を見付けて，対処できるようになっているか

⑩ プログラムの過程と結果を文書にして残してあるか

このうち，①はプログラムの責任をコンピュータの中でいかに分割し，実際

の処理に当って，それをいかに適合させるかということであって，⑧，⑩と共にもっとも重要な項目のひとつである。

システムの可監査性の原則としては，

① システムは健全か（信用できるか）

② 適切な統制がなされているか

③ 処理の流れが追求できるか

④ 目に見える監査証跡があるか

⑤ システムが十分文書化されているか

⑥ 文書が更新され，すぐに検索できるか

が挙げられる。①は特に実際にシステムを使う時に，情報や自分の要求するものを入れて，その要求に従った答が出て来るかどうか，つまり，入るものと出るものとが適合しているかどうかを知ることが重要である。

統制の３つの型を挙げると，

① 間違いがあればプログラムを止めてユーザに知らせる

② なぜ止ったかの理由を明らかにする

③ その間違いをプログラム自身で修正する。

このうち，③は他の２つに比べて遙かに多額の費用がかかる。

ＩＢＭでは，監査人の養成について特に１日の勉強コースがあり，統制と可監査性について研修が行なわれている。

3. 情報システム統制改善のための実施要領

ＩＢＭにおいて，システム安全保護相談員というのは会社のスタッフであって，データの安全保護とシステム統制に関する顧客からの要求に対して，それを製品に反映させることを仕事としている。

安全保護の問題やシステムを濫用するという問題は，無い事が望ましいことであるが実際には存在する。しかしＩＢＭではこれらの問題に対して，特に犯罪を前提としてシステムを作るということでなしに，情報を外に洩らさないという事

を中心に考えている。

現在，米国では４百万の端末があり，それを使う個人や機械の独立性も重要であるが，それ以上に端末相互間および端末と使用者との関係が重視されている。

コンピュータを使う企業の経営者，管理者，実務担当者の間での，コンピュータに関しての意思疎通が重要である。彼等は，企業を経営するにはコンピュータの専門家でなければならないのか，統制をより厳しくする必要があるか，コンピュータを過信してはいないか等の疑問を持っている。日本でも米国でもコンピュータの濫用は非常に危険視されているので，これを防ぐための法律や社内規則等が作られる。

コンピュータを使用する機関の経営者同士，また端末の使用者同士では，これらの問題について色々と話し合われており，コンピュータの利用価値，犯罪の防止，使用上の取り決め，個人秘密，統制および監査について情報の交換がなされている。

(1) 安全保護

安全保護とは本来，データを事故，災害および意図的な破壊や改変から守るすべてのことを含むのであるが，現在ＩＢＭで行なわれている調査，開発においては，個人的，物理的環境，災害からの避難等はその対象としていない。これらは各企業によって異なり，それぞれにおいて対処すべき問題と考えるからである。

安全保護は次の４つが基礎となる。

① 火災や盗難から護る

② 必要以外の人が使うことを防ぐ

③ 使う人の責任を定める

④ 誰が情報の所有者であるかを明らかにする

このうち，②③④は類似しており，相互に関連が深い。

まず最初は，水などの災害からデータを護ることから始まり，次第に高度な次元での問題を取り扱うようになってきた。

データ管理は，それを扱う人間の関係が最も重要であり，またそれぞれが使う端末間の情報の流れが重要である。

情報について，①誰が所有するか，②誰の責任で管理するか，③誰がその権限を持つか，という３つの観点から述べる。

この問題について，ある欧州人は，次の５つに分けて説明している。

① 情報の主体

② 情報の作成者

③ 情報の管理者

④ 情報の使用者

⑤ 情報の関与者

データがどのように，必要な範囲で流れるか，を理解することが大切であり，それが企業の利益につながるのである。

さきに挙げた３つの観点は，①安全保護，②可監査性，③システム管理，の問題なのである。

まず，安全保護とは，データをどのように護るか，つまりデータを使う権利のない人から護る，権利のある人でもその人の冒す事故から守る，また自然の災害とか，故意の妨害や破壊から護ることである。

誤操作やシステムの誤り，退職従業員による悪意のデータ消去，火災，水害，暴力等がその対象である。外的要因は色々考えられるが，特に基本的なことは，人的要因による誤りや失敗を防ぐことであり，人物鑑定，授権，強制，記録，会計統制，編集統制などが方策として考えられる。

また，その手段としては，検索統制，整合性，暗号化等がある。

特定の権限を持つ者しかシステムに近付けないようにし，その権限は，データを，①読む者，②利用する者，③更新する者，④流す者に分けて決める。パスワードを使ったり，権限のない者が触れると警報が鳴ったり，データを暗号化したりする方法が効果的である。

ＩＢＭで開発した暗号化の方法は，1977年に連邦政府によって標準として

採用された。暗号化すれば，データが盗まれることも防げるし，また正しくないデータが入り込むことも防げる。

しかし，安全保護には完全なものはなく，また費用が多くかかるものであるから，損害が発生した場合の損失と，それを防止するための費用との兼合いが重要である。

(2) 監　査

データの不正使用，不当なデータの混入，処理の誤り等を発見するには監査が必要である。

ここではシステムの変更に対してどのように柔軟性を持たせるかが問題となる。

ソフトウェアの監査は，監査人とシステム設計者とが協力して実行する。

個人の秘密を守るための法律は国によっても，州によっても異なるので注意しなければならない。

(3) システム管理

システムの統制には次の6つの型がある。

① データの入出力についての統制

② プログラムの準備，検査，提案についての統制

③ 会計的な統制

④ データの蓄積および保管の統制

⑤ 失敗の回復と再稼働の統制

⑥ 回線網通信の統制

このうち，⑥は，いつも決められた時に情報が流れて来るかの制御である。

以上述べた，安全保護，可監査性，統制，の中で，現在では最後の統制にあまり注意が払われていない。これは，設備，プログラム，人間にいずれも限界があり，あと回しにされているからである。

これらの問題について，これからどうして行くか，統制については，責任と権限をどう割り当てるかが重要である。

安全保護については，何に対して護るか，如何にして護るか，をよく知ることが重要であって，そのためにはシステムをどう変えて行くかを判断しなければならないのである。

4. 監査ソフトウェアとしてのＩＢＭ製品

コンピュータ・システムのソフトウェアは，個々の業務をサポートする適用業務プログラムから，機械に近いオペレーション・システムまで，いくつかのレベルに分れている。

監査の機能を果すものとしては，適用業務プログラム自身に組み込む方法と，監査のための独立したプログラムとがある。昨年の９月に調査して，ＩＢＭのプログラムの中で監査の機能を持つものをまとめてカタログを作ったので，その中からいくつかを紹介する。

ADRS Ⅱ（A Departmental Reporting System Ⅱ）

ＡＰＬ言語を基礎として作られているが，使用に当っては必ずしもＡＰＬの知識を要せず，記述が易しく使い方も簡単である。

これでデータを整理して，例外的な事象を見付け出すとか，行列的な取扱いが容易である。

TPNS（Teleprocessing Network Simulator）

テストデータを自動的に作るとか，ネットワーク自身をシミュレートできる機能を持っている。システムの実行前の文法的テスト等，繰り返す時に非常に便利である。

SMF（Systems Management Facilities）

監査に必要な諸データを自動的に収集して記録する。例えばＩＰＬの回数，機械のコンディション，ストレージの使用状況，補助記憶装置のデータ，ＣＰＵの使用率などの基礎データを集めて編集し出力する。

システムライフの見積り，大型機へのリプレースの時期などのシミュレーション等にも使える。

RACF（Resource Access Control Facility）

コンピュータ資源へのアクセスを直接に制御する機能を持つ。

ＭＶＳ等の大型システムでは必須のものであって，セキュリティのレベルの構成や，トライアルが簡単にできる。

Source Compare／Audit Utility

プログラムが指定通りにコーディングされているか，順次に比較してチェックする。特定のカラムだけに注目して追うこともでき，また特定のフィールドに対するアクセスのセーフガードにも使える。

この他，Audit File やAudit ―Source Code Compare 等内部監査のために作られたプログラムが，特に重要である。

このカタログはまだ初版であり，次第に充実した内容に改版して行くつもりである。これは，内部監査人にとって有用であるが，システム部門にとっても，監査部門からの問い合せ等について使える。

（質問）　このように沢山の監査プログラムがありながら，端末からの操作等によって色々と不正等が行なわれた事例が多く聞かれるのはなぜか。

（答）　監査プログラムを現実にどの程度使われているかは疑問であり，またそれが監査人にうまく使いこなされていたかどうかが問題である。しかし，実際にはそう多くの事故が発生しているわけではなく，興味本位で大きく報じられている場合が多いと思う。

Ⅲ．マサチューセッツ工科大学

1. セキュリティ研究の概況

分散処理システムの保護について，MITは5年前から研究を行っている。近年，技術進歩により，高機能のパーソナル・コンピュータが，個人や家庭にも普及するようになり，分散処理システムにおけるセキュリティについて，新たな問題が発生して来ている。MITでは，過去にMULTICSシステムを開発しており，セキュリティについては強力な機能を持っている。

MULTICSのセキュリティは，Kernel(os)によって全てが行われている。図2に示すように，端末からのユーザ・プログラムへのアクセスは，全てKernelを通して行うようになっている。

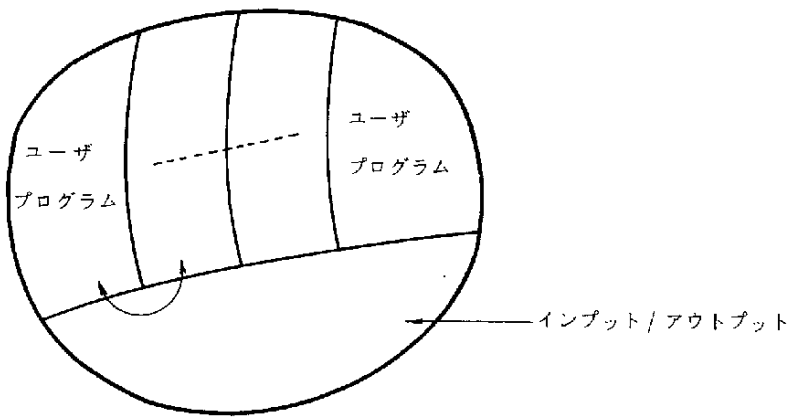


図2　MULTICS Protection

分散処理システム（図3）のようにネットワークで接続されている場合，Kernelで保護を考えると，概念的にはKernelと，3つのコンピュータを接続することが考えられる。またKernelを通し，パーソナル・コンピュータが，相互に相手のプログラムを利用する事もできる。しかし，実際には，ネットワークの保護措置を組込む事はむずかしい問題である。従って，ネットワークを通して，2

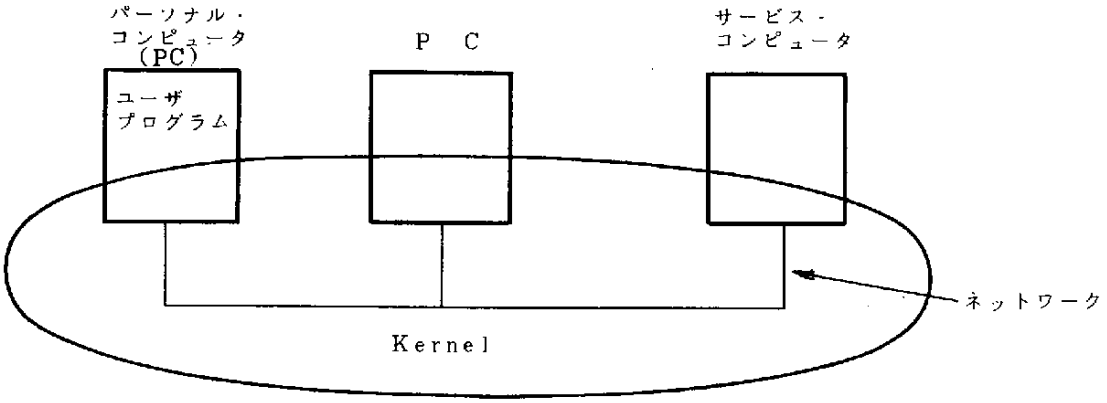


図 3　分散処理システム

つのコンピュータの連絡を保護するために，暗号の適用が考えられている。

2. 暗号化技術

メッセージを送る時に，特定の受け取る人にしか解らない暗号を使って送る方法がある。

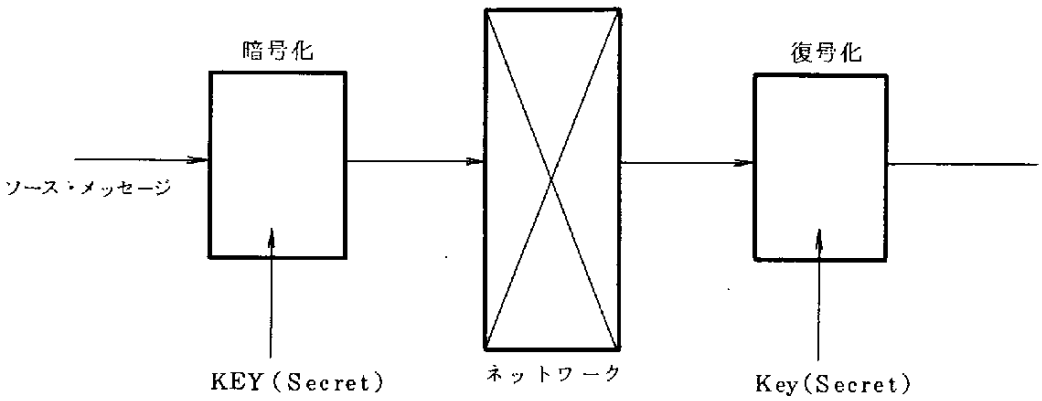


図 4　暗号化技術

図 4のように，ソース・メッセージを送る側で暗号化し，ネットワークを通し受取る側で暗号を解読し，メッセージを受信する方法である。従来はオリジナル・メッセージをネットワークを通して簡単に送れるようになっていたため，ネットワークの途中で盗聴されてしまう可能性もあった。

現状では，図４の方式で保護するように研究が進められているが，完全に保護出来ると言うまでには致っていない。

重要な問題は次の３つである。

① 未承認の読み取りからの保護

② 未承認の修正・変更からの保護

③ エラーや犯罪に対する責任の確立

(1) ＭＩＴにおける研究内容

ＭＩＴでは，上記についての対策を現在研究している。

① 未承認の読み取りについては，KEYが暗号であれば保護として有効であり，問題はないと考えている。

② 未承認の修正・変更については，図５のように，送る途中で違う暗号やメッセージを入れ替えたり，オリジナル・メッセージの暗号や内容を修正したりされても最終の受信側では解らない。

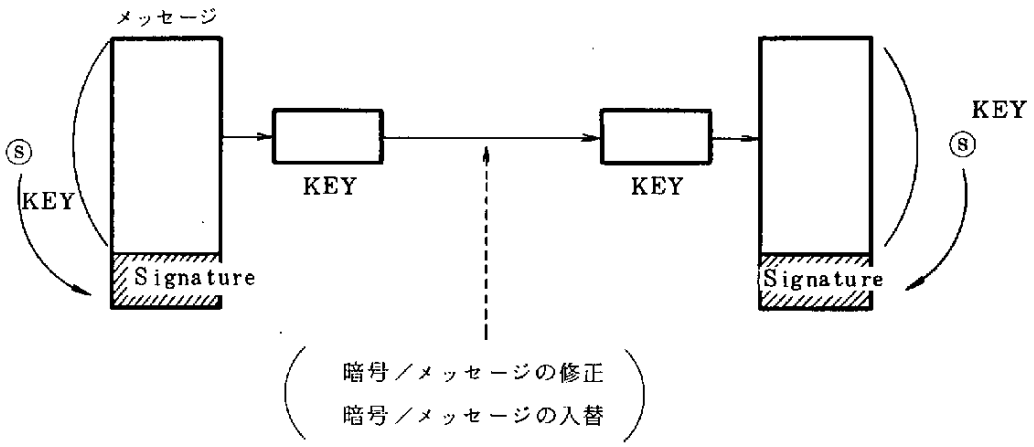


図５　Signature を入れた暗号化

このためには，現在研究中であるが，オリジナル・メッセージにSignatureを使い，メッセージに追加して暗号を作る事を考えている。受信側では，Signatureを解読することによって，オリジナル・メッセージである事を判別出来る。もちろん受信側では，相手のSignatureを解っている必要が

ある。

もう一つの問題は，図６に示すように，メッセージを途中で誰かが盗ってもう一度入れた場合，Signature を付けておいても受信側では解らない。

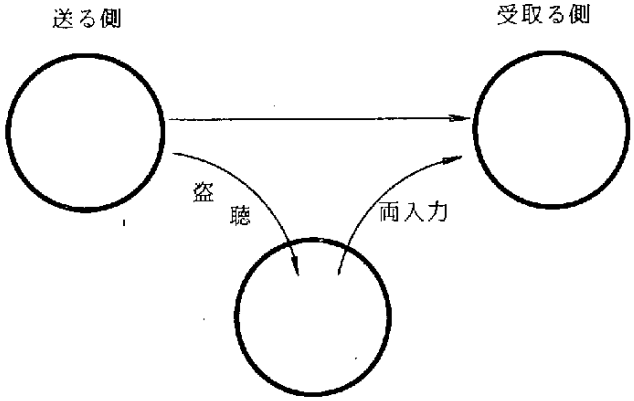


図６　再　入　力

これについては，Idempotent（数学用語で同じ事を２度行っても有効とならない）の確保を研究中である。基本的には図７のように，メッセージに時間を入れて送り，受信側よりメッセージを送り帰して，その時間に確かに送ったかを確認する方法がある。

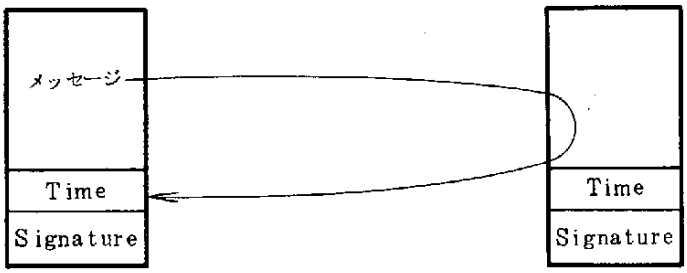
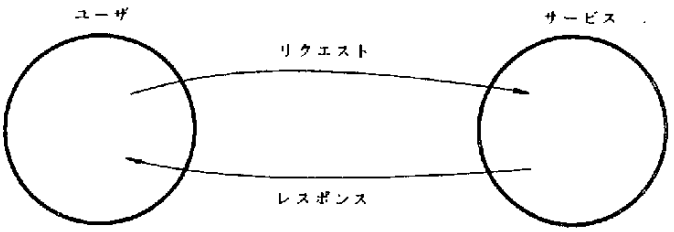


図７　Idempotent の確保

③　エラーや犯罪に対する責任の確立については，人間がコンピュータの操作にからんでいるため，色々と問題となる。

あるファイルに，ユーザが登録したデータをコピーして貯えておいた時，数ケ月後に内容が変えられていた例がある。これは，故意にやられた時は防ぐ方法はないが，誰れがやったのかを調べる必要がある。また誰れが，故意や偶然によって起したのかは，Signature を使って調べる事が出来る。

これから研究しようとしている基礎的な考え方を図8で示すと，



（情報露呈の問題
間違いの立証）

図8　今後の研究課題

ユーザとサービスの間で，リクエストとレスポンスのやり取り上で，トラブルが発生したとき，

a　問題を見付ける事

b　問題がユーザなのか，サービスなのかを切分ける事である。これが十分に出来れば，法的な処置や管理上の対処が可能となる。

暗号の場合はトラブルの発見は出来るが，問題の所在の切分けが出来ない。

ユーザからのリクエスト，Signatureを全部ユーザに送り返してやれば，自分の要求した内容か，要求した回答かを，ユーザはすぐに判断出来る。この事から，ユーザは誤りをすぐ発見出来るため，トラブルが発生して裁判になっても証明出来る。これをContract（関係を明確にさせることの意）と言っている。

この場合一番重要なことは，特定の人にしか読めないKEYである事である。KEYがユーザまたはサービスによって公開されてしまえば，全て意味をなさない。従って，研究を一歩進める上で，KEYを外に出さない工夫が必要であり，研究はこの段階で止まっている。どのようにしてKEYを隠し続けるかが問題である。MITでは，ファイル・サービスをするSWALLOWシステムを持っているが，これによって保護に関する種々の実験を行っている。

(2) Authentication サービスについて

分散処理システムを，今後は１つの世界的な規模として概念的に考える。コンピュータ通信が，どのコンピュータ同志行われたのか，送る人と受取る人が，KEY と Signature を解っている場合は問題ない。図９に示すような Authentication サービスを想定する。

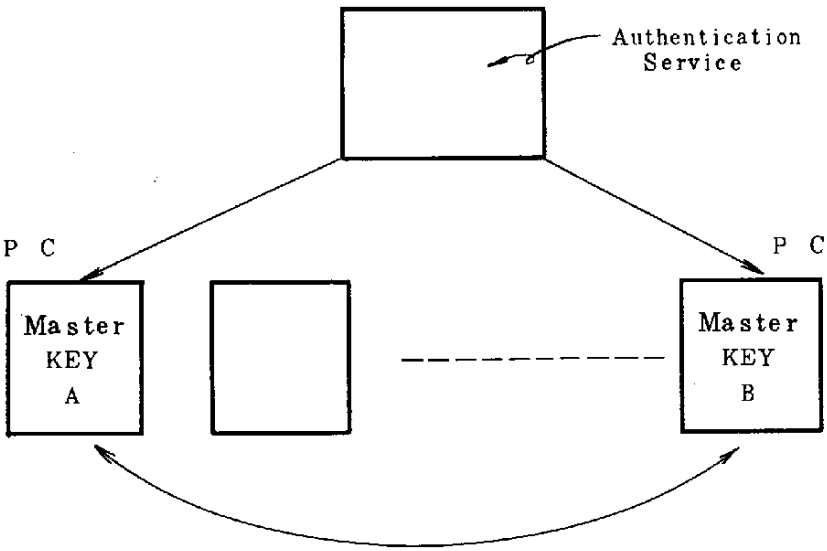


図９　Authentication サービス

これは互いのＰＣ（パーソナル・コンピュータ）を紹介する様な機能を持っており，電話帳の役目をする。

各ＰＣは各々，異なるマスター・キーを持っており，Authentication サービスが全てのマスター・キーを把握している。各々のＰＣは，互いのマスター・キーを知らないので，Authentication サービスを通さないと通信出来ない。各コンピュータは，Authentication サービスとは暗号と Signature による通信がいつでも出来る。従って，秘密の守れる，信頼性のある通信が可能になる。

この場合は，各コンピュータ同志の保護は問題にならず，Authentication サービスと各コンピュータ間の保護措置をどうするかにしぼられる事になる。Authentication サービスを複数組合せる事により，より機密の高いプロテク

トが出来る。

これらの研究は，次の人がやっている。

UCLAでは　Popete 氏

XEROXでは　Needham 氏

Schoulder 氏

Dr. Read は，Authentication サービスの運用方法について研究している。エレクトリック・メール・システムや，リモート・ターミナル・アクセスに適用する事を考えている。要は複雑に見えるものでも，簡単に操作出来るようにすることである。

これらの他に，人間の Identification についても問題になって来ている。これには，自分だけのKEY を持った暗号だけを入れておく Pocket-Computer がつくられている。ペーパーバック・サイズである。

Ⅳ. マサチューセッツ生命保険会社

1. 会社概要

当社は，総資産70億ドルで，全米第10位の生命保険会社である。監査部門を組織で示せば次のようになる。

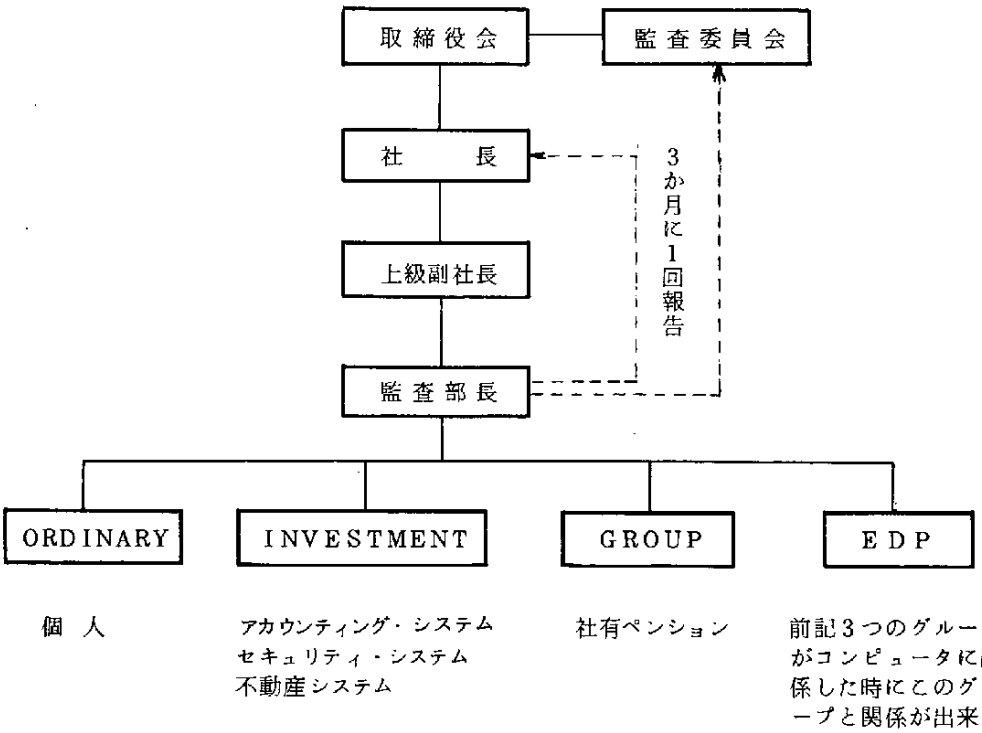


図 10　監査部門の位置づけ

内部監査人の員数は次の通りである。

1978年：20人（システム監査人 11人）

1982年：27人（システム監査人 2人）

システム監査人の主要業務は次の通りである。

① ＤＰ部門に対するコンサルタントとアドバイス

② ＥＤＰに対する新技術の採用

③ 文書に対する責任

2. コントロール・ガイドライン

1977年にコントロール・ガイドラインを作ったが，これだけでは不十分であった。

監査する場合にはいくつかの問題が発生していたが，これはデータ・プロセシング（ＤＰ）部門の人達が監査の意味を良く理解していなかったからである。したがって，ＤＰ部門の人とユーザには監査について，監査人に対してはＤＰ部門から出た出力を理解させる教育を行なった。

1978年には，上級管理職にはＥＤＰの講習を行ない"Auditing Computer System"のドキュメントを作成した。これは他社で作ったものを許可を得て当社に会うように作り直したものである。

内容は下記の項目より構成されている。

- Introduction
- Audit Approoch
- Auditing an Application
- Tools and Techniques
- System Design Audit
- System Conversion
- Program Changes
- Control Guidline

コントロール・ガイドラインの項目

(1) Procedural Controls

A. Input Controls

B. Processing Controls

C. Output Controls

D. Control of Systems Using Direct Methods

E. Data Retention

F. Error Control

G. Data Change Control

H. File Security

(2) Administrative Controls

A. Program/System Documentation

B. Program Change Control

(3) Organizational Controls

A. Separation of Duties

B. Management Trail

上記の項目全てを使用するのでなく，ＤＰ部門はユーザとか監査部門の人と話し合い，どのコントロールを使用するか考える。監査人はこれを勉強してどれがこのシステムに合っているかさがし出さなければならない。

3. システム開発ライフサイクル

システム開発のライフサイクルは次の通りで，①から⑪の場所で監査人が参加する。（図11）

監査人のチェックの重要度および参加する比重は次の通りである。

活動項目	ライフサイクル項目	重要度	監査人の参加度
①，②	Project Cycle Phase	小	1(%)
③	Feasibility study	小	2
④	Systems analysis and design	小	8
⑤	Detail design	大	40
⑥	Programming	小	1
⑦	System test plan	中	10
⑧	Unit test	小	3
⑨	User Procedures	小	5
⑩	System test	中	15
⑪	Conversion	中	15
	合　　計		100(%)

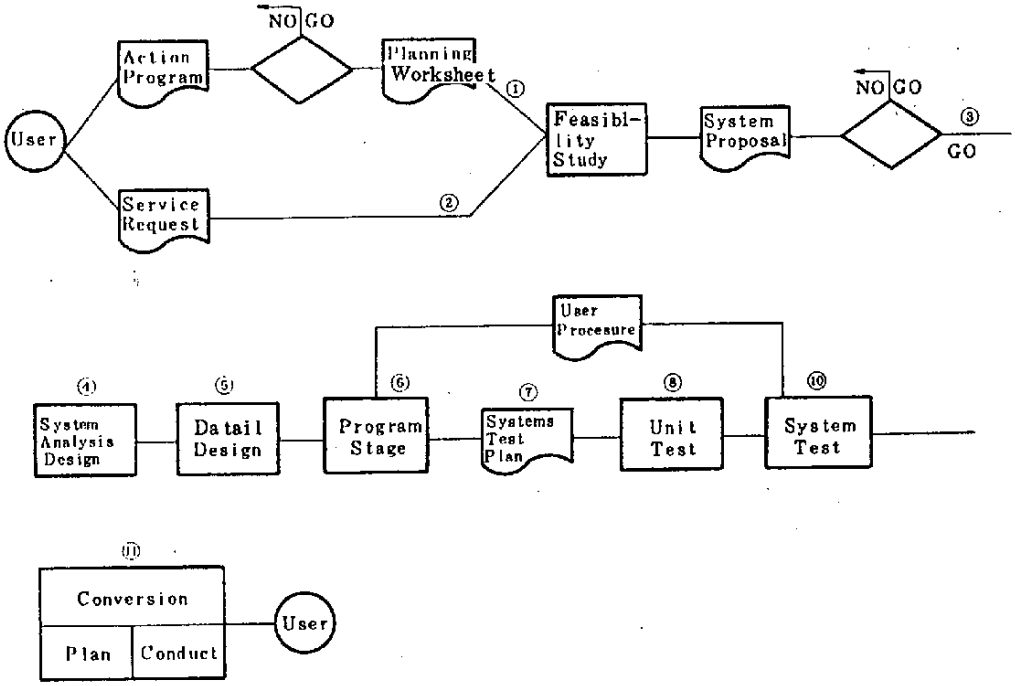


図 11　システム開発ライフサイクルと監査の関与

上記のように，監査人はプログラミングの段階ではあまり参加しないが，ディテール・デザイン，システム・テスト，コンバージョンの段階で参加をする。

③では，ユーザは使用システムを決め，効果と使用の可能性を検討し，提案書を提出し，関係者で使用するかを決め，システム・アナリシスの段階に入るかどうか決める。（毎年８月１日までに次年度の使用システムを提案する）

④では，コンピュータの規模等を決める。

⑤では一番時間をさき，会社の利益を考えて設計する。

(1)　Auditor's　Spec Review（文書例）

Date _____

External Review　　（他部門のマネジャのコメント）

Internal Review　　（担当段階のコメント）

Team Review

Design Decision

System ：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Task ：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

Comnents　上記の４項目全てがチェックを終ると持ち帰り最終コメントを監査人が書き込み最終保存版とする。

Auditor's signature

(2) Specification Summary Sheet（文書例）

A System：

B Function：　　C Control code

D Specification Titles／Log Book No：（監査人が要約する）

E Object of Function：

（いらないもの良くないものを書き出す）

F Overall Opinion：（監査人のシステム全体の意見）

G Open Items／Follow-up Planned：

（わからないところ，問題点を書き出す）

H Special Actions Taken：

（特にしなければならないことを書き出す）

I Data Retention：

J Fusure Audit Considerations：

K Reference：

（現在のシステムとインタフェースが合っているか書き出す）

L Other Comments：（いままで書けなかった項目を書き出す）

Prepared by：＿＿＿＿＿＿＿＿

Date：＿＿＿＿＿＿＿＿

このディテール・デザインの段階では，監査人はこれで良いという答まで出さないでコンサルティングとアドバイスだけする。

しかし最終的には，監査人はここで書いた文章には責任を持たなければなら

ない。この段階で疑問が生じた場合，徹底的に検討して書かなければならない。そうしなければ，システムを開発し運用した場合，会社側の大きな損害や，政府から余計な税金をかけられるような事態に発生する。監査人は，スケジュール通り仕事が行なわれ，正しいシステムが出来るかどうか調べ，詳細まで把握しなければならない。

ここでは一人の監査人が書くが，この文章を見ると，一見して全容がわかるようになっている。

サマリーの報告ルートは，各グループと監査人と一緒に作成し，各部門のマネジャに報告したのち，監査部長に報告する。

⑥は監査人は参加しない。

⑦はレビューするだけであり，システムが正しく動作しているかチェックする。

⑧は参加しない。

⑨はユーザ・テストに関与する場合の手順を決めるが，監査人はその手順が正しいかどうかチェックする。

⑩はユーザの人が中心となるが，監査人はシステム・プラン通りテストしているかどうかチェックし，この結果から社長に有効であることを報告する。

⑪は旧ファイルから新ファイルに変更する際，正しくされたかどうかチェックする。

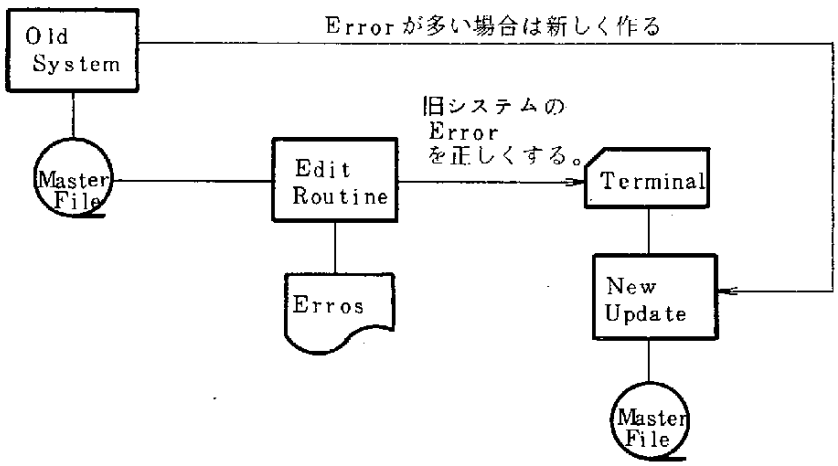


図 12　コンバージョン

(3) レポートの種類と内容

① Finding （問題点） 監査人とＤＰ部門の人と検討した項目

② Recommendation（試案） ２週間位で作成

③ Response（解決） 監査人は合意項目として作成

上記の３つのレポートを社長に出すため解決過程がはっきりする。

V　ドン・パーカー・セミナー

1. 概　　要

サンフランシスコの南，およそ30マイルのメンロパークの一画に広大な敷地と緑の芝生と木立に囲まれてSRI INTERNATIONALがある。まさに研究所としては理想的な環境にあり，政府関係あるいは民間企業より委託されたテーマについて研究開発を行っている。

ドン・パーカー氏は，大学にて数学を専攻し，以来コンピュータに関係してきた。コンピュータ・セキュリティに関しては，1965年にＡＣＭ（Association for Computing Machinery）のために，「専門家のための行動基準」を書いた時に始まる。1970年，全米科学財団（National Science Foundations）の補助金を得て大掛りな調査を行い，その結果をまとめた報告書「コンピュータ濫用」（Computer Abuse）は各方面から高く評価された。

最初の研究計画書には，コンピュータ犯罪（Computer Crime）という言葉を用いていた。しかし法律専門家より異議があり，コンピュータの反社会的使用（Anti Social Use of Computer）というタイトルを使い出した。これもまた，社会学者からの異議があり，結局コンピュータ濫用（Computer Abuse）という言葉を創出した。現在では，この言葉は彼のトレード・マークというべきものになっている。

なお，同氏がみつけたコンピュータ犯罪の第一号は，1966年10月18日火曜日のミネアポリス・トリビューン紙の第1面に出ていたそうである。

2. コンピュータ犯罪・濫用について

(1)　コンピュータ犯罪を問題にする理由

現実の問題は，エラー（事故）による損害の方が，意図的によって被る損害

より多大である。しかし，その解決策はどうかと言うと，「意図的な行為に対する解決策は非常に難しい」のである。

つまり，次の点の意識が必要となる。

○　意図的な行為に対するセキュリティ対策は，事故のような意図的でないものに対して効果がある。

○　事故的な損失に対するセキュリティ対策を実施しても，意図的な行為に対しては役立たない。

日本においては，プログラムに対しての特許や著作権は認められておらず，複製を防ぐ手段のない事が問題である。日本の警察関係者の話では，「日本ではＭＴを盗んだとしても，そのＭＴの値段が15ドルならば，15ドルのものを盗んだとして罰せられる。仮に，そのＭＴの中に30万ドルの価値の情報が蓄積されていても，30万ドルの価値情報を盗んだ事にはならない。」

これらの防止のためには，立法化が必要である。現在アメリカでは，13州でコンピュータ犯罪防止法が成立している。

3. コンピュータ犯罪のテクニック

(1)　トロイの馬

プログラムの中に「トロイの馬」 ― つまり作為の命令を紛れこませ，システムが正常に働く中で同時に犯人の意図した事を行なわせるやり方である。何億というプログラム命令の中に僅か数個の作為が混入された時，それを発見するのはほとんど不可能に近い。

(2)　サラミ・テクニック（ Salami Technic ）

サラミを薄く切ったものを何枚となくたくさん集めるようなもので，１回当りの被害は僅かで目立たないが，少しづつ何回となく繰返し，いろいろなところから金を盗る手口。

(3)　ロジック・ボーム（ logic Bomb ）

あらかじめ設定した日とか，時間に動作するように「トロイの馬」を忍びこ

ませておく方法。

(4) スーパーザッピング（Super Zapping）

使用する権限がないのに偽ってユーティリティ・プログラムを使用したり，妥当性を装ってプログラムを無力化させる手法。

(5) 盗聴（Wire Tapping）

今年日本で発生した回線盗聴事件は，世界で二番目の事件である。最初はアラスカで発生したもので，石油会社が石油採掘権の入札価格を盗まれ，競争会社の入札に僅かの差で敗れてしまった事件である。

(6) その他

・Data Diddling（インプットデータの改竄）

・Data Leaking （アウトプットデータの漏洩）

・Trap Door Usage

ハネウェルのマルティクス・システムは，これらのセキュリティについて，世界で一番強い計算機である。ＩＢＭのＭＶＳは比較的防御に強いシステムである。この二つのシステムは，これらの犯罪を防ぐ思想を取り入れて設計されている。

4. コンピュータ犯罪の分類

コンピュータ犯罪についての統計がいろいろ出されているが，それらは必ずしも実際に発生した件数を表わしているものではない。図13はアメリカにおけるコンピュータ犯罪の調査報告件数である。これらの調査を行っていく中で，以下の点が問題である。

・ 情報源は新聞であり，新聞は読者の興味のある内容をのせやすい。

・ 内容が正確性にかける。（損害を受けた者が新聞に対してはあまり内容を語りたがらない）

(1) コンピュータが対象物となるケース

コンピュータそのものが対象物となって損失を発生させるものであり，ハー

ドウェアの破壊等はこのケース。（図 14 ）

(2) コンピュータが損失を生む環境を創り出すケース

コンピュータがなければ発生しなかったかもしれないが，コンピュータがあるために，それを利用して損失を発生させる。例えば，データの窃取，あるいは不正なプログラム・コピー等。（図 15 ）

(3) コンピュータが道具に使われるケース

コンピュータを犯罪の道具として利用するケース。他人の金銭，資産などの盗みはこのケース。（図 16 ）

(4) コンピュータが象徴として使われるケース

コンピュータが脅迫やゴマカシのための象徴として使用されるケース。（図 17 ）

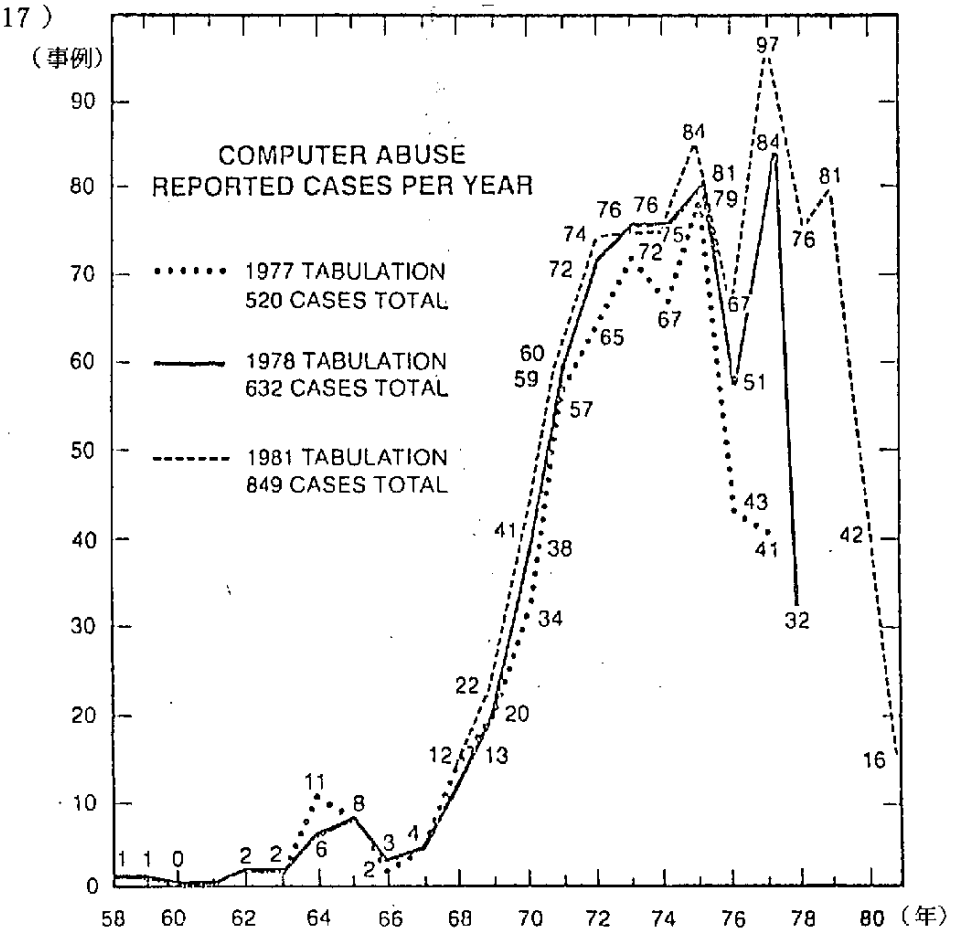


図 13　コンピュータ濫用事例

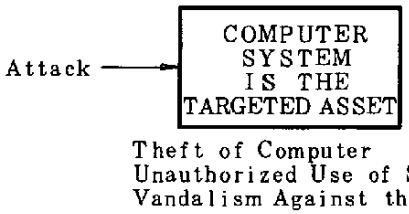


図 14　コンピュータがアタックの対象

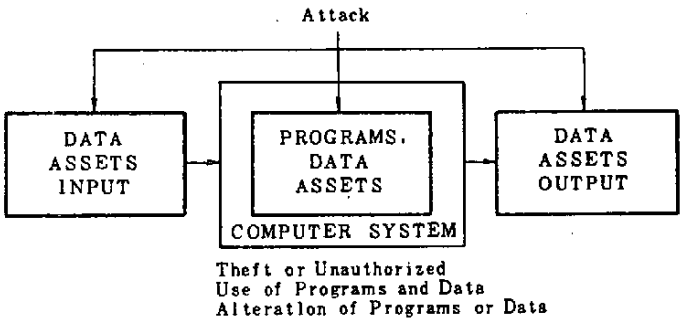


図 15　コンピュータが犯罪環境を生み出す

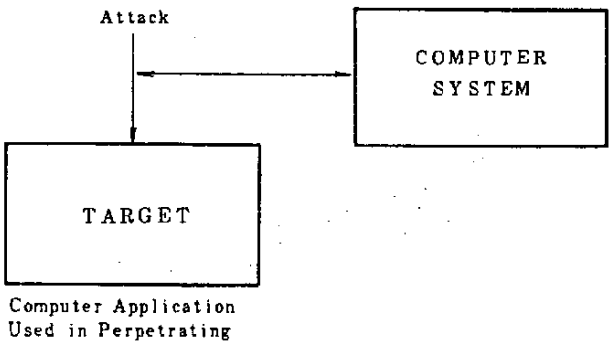


図 16　コンピュータが犯罪の道具

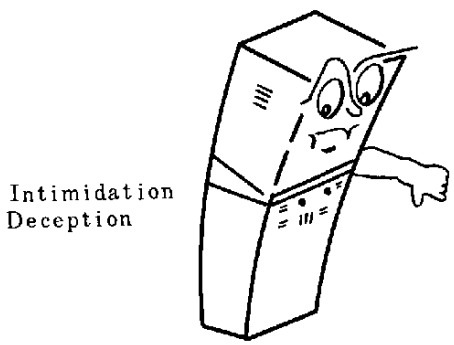


図 17　コンピュータが犯罪のシンボル

5. コンピュータ犯罪の犯人像

コンピュータ犯罪者にインタビューし（30ケース），その人物の分析を行なったところ，以下の特色があった。

- 理想的従業員
- 素人のホワイトカラーの詐欺師（但し最近はプロとして行うものが増えている）
- 詐欺師でないと確信されている人
- 分割できない仕事の担当者
- 信用ある地位にいる人
- 大きな権限をもっている人
- 好奇心やゲーム的感覚による動機
- 若　さ
- 人を傷つけない
- 他人のすることをするだけの人
- 他人の助けを必要とする人
- 予期せぬ暴露に対して不安を持っている人
- 監査人の行動を予期し打ち負かそうとする人

6. コンピュータ・セキュリティ上の問題点

(1) LACK OF MANAGEMENT SUPPORT

- 上からの指示を無視するような事をさせてはいけない。

(2) マジノライン・シンドローム

- 犯罪を実行しようとするものはシステムの盲点を知っており，そこをついてこようとする。

(3) SUBOPTIMIZATION

- コンピュータに対するセキュリティも大事であるが，それ以前にデータを

作る所や保管されている所にも，セキュリティをおかなければならない。

(4) 過度のセキュリティ・レビュー

- 余計な資金や時間をリスク・アナリシスに費やす必要はない。
- ある程度のリスク・アナリシスはすでに達成している。

(5) 技術シンドローム

- 犯罪を行うのは人間であり，人間管理の問題を無視してはいけない。

(6) セキュリティ作業におけるセキュリティの欠如

セキュリティを実施する人間に対して，セキュリティを確実に実行させる。

- ドキュメントの暴露
- ルーズなおしゃべり
- 特権的な行動

7. コンピュータ保護のための問題点

(1) ハードウェアの保全

electric modification に関しては，完全なプロテクトが行なわれている。

(2) ソフトウェアの保全

ソフトウェアが仕様書通りに動作することの証明として

- 数学的に立証する
- テストによらなければならない

の両意見があるが，両方を併用して立証するしかないであろう。

(3) ＩＤの確認

資格の確認

データベースへのアクセス権のレベル化

多くは暗証番号を利用しているが，最近スマートカード（マイクロチップを持つカード）の利用が考えられている。

ＳＲＩでは，コンピュータペンというものを開発した。これはペンの筆圧，

水平面での動きを解析して，本人確認を行っている。その他の方法として，手の形，指紋，声紋の利用が考えられる。

(4) 暗号キーの管理

昨年，アメリカでは，暗号化装置が1,500万ドルしか売れず，モトローラ社は最近この機械の製造を中止した。

暗号化装置が利用できない理由は，一つは暗号化における鍵の管理が解決されていない事，およびコストが高いことである。（スタンフォード大学のDr. Martin Hellman はＤＥＳ方式の暗号解読について一日で可能であると言っているが，政府関係者は91年間かかると主張している。）

ただし，ビジネス用としては，ＤＥＳアルゴリズムは十分に利用できるという事であった。アメリカにおける銀行での利用は，連邦準備銀行が採用するまでは利用されず，今後５～６年間はないと考えられる。（暗号鍵のマネジメントが統一化されていない事により，問題が多い）

(5) 小規模システム

大規模システムでは，開発においても作業分担がなされ，セキュリティ対策にもなっているが，小さいシステムでは一人でいろいろな作業を行っている。この為には，デュアル・コントロールを利用すればよい。

(6) 分散システム

(7) 行動のインタフェース

(8) 従業員に対する援助

(9) 従業員に対する訓練

(10) 消極的保護策

8. 人間を中心にした安全性

人間の行動および責任を，技術面，手順面から管理していく事は，コンピュータの安全性を考える上での基本である。

つぎにあげるものは，ＳＲＩが推薦していることである。

① 専門職のもたされている責任とは何かを，各従業員に明確にさせる。

② 行動規定を順守させる。

③ 従業員に関して，バックグラウンド（個人の経歴等）を良く知る。

④ 薬（麻薬）の服用，飲酒，賭博，個人の財政，家族のことに対して，相談にのって解決させるためのサービスを行う。（こういう履歴のある人間がコンピュータ犯罪を起しやすい）

⑤ 勤務評定や賃金評定の中にセキュリティについて守っていることの評価を入れる。

⑥ セキュリティに関してのビジネス・ポリシーやその順守の方法について明確にしておく。

⑦ セキュリティに関しての訓練やテストを強化しておく。

⑧ リスクの高い仕事に従事するＥＤＰ要員に対して，免許や認定を与える。

9. リスク・アナリシス

一般的によく言われているリスク・アナリシスは，次の式で表わされることが多い。

Expected loss = P × A

If P is acts per year and A is loss in dollars, then

Expected loss is expected annual loss in dollars.

P = Probability of a loss act

A = Amount of possible loss

ただし，ＳＲＩの分析では，定量的リスク・アセスメントは問題がある。

① 包括的な定量的リスクのアセスメント（金額や発生頻度）は実際的でない。

- コスト的に見ると効果的でない。
- 満足できるほど正確でない。
- 前例を再使用できない。

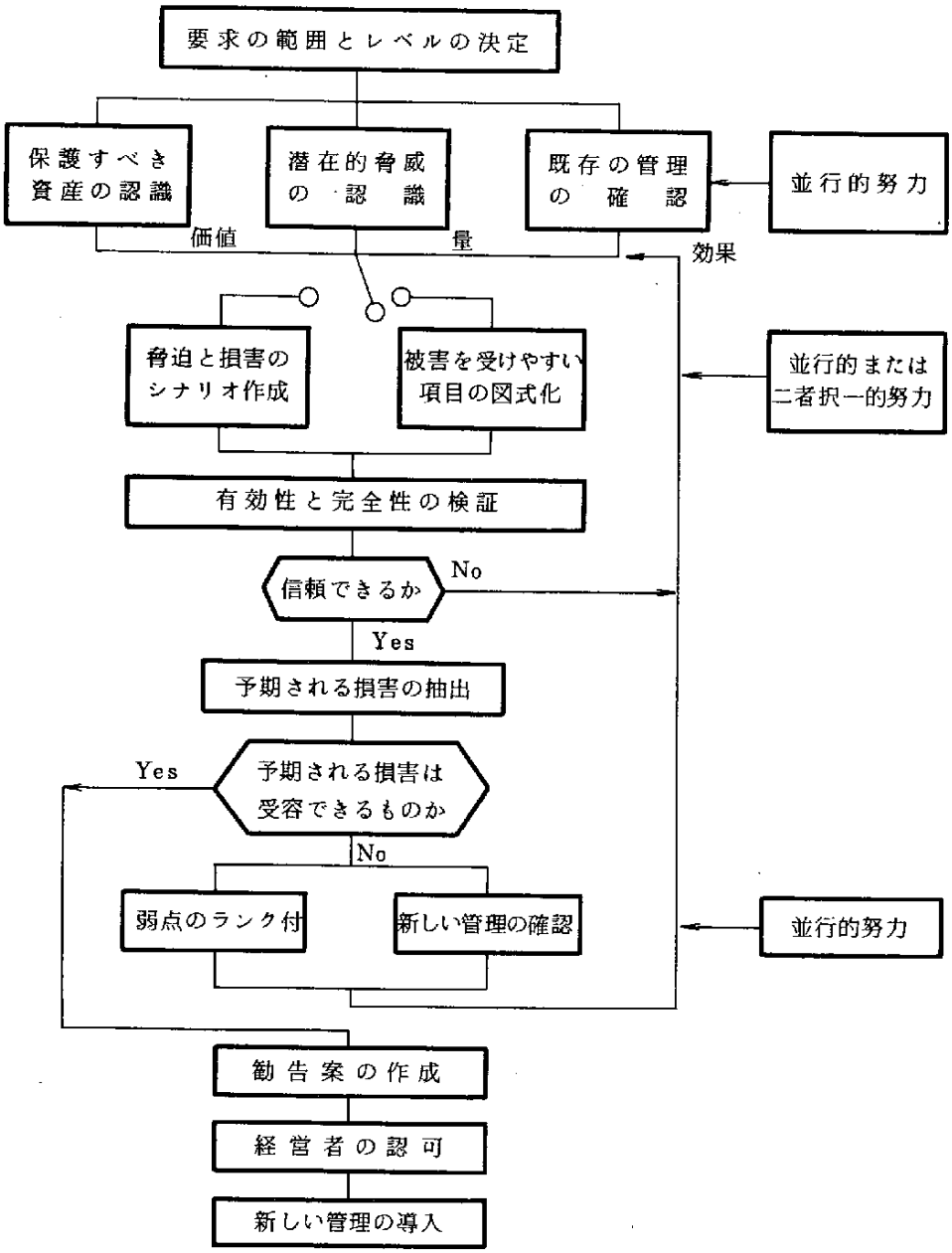


図 18　リスク・アナリシスの方法

② 以下のような，限定した範囲でのアセスメントは有効である。

- 被害の受け易さの比較
- 高額費用が必要な保護策の選定

- 新しいセキュリティの問題

③ 以下の点に基いた定性的なリスク・アセスメントが勧められる。

- 経験豊かな観察と聴取
- 経　験
- 一般的な実践
- 一般的に有効な保護策

10. 基本的なセキュリティ・コンセプト

過去に行なわれた犯罪を参考にして，その防衛方法を考えたり，今までに行なわれている防御の方法を利用することがよい。

例えば，次の方法がある。

① 人格のテスト。

- 似たような環境下で他の人々がすることを調査する。
- 合理的で有効なセキュリティ製品を利用

② 以下の項目は保護策の例である。

- 安全ドア
- バッヂの着用
- パスワード
- 消火・防火設備
- ファイルの使用の管理
- 暗号

③ 次の事項は，一般的にすでに行なわれており，リスク・アナリシスは必要ない。

- 偶発事故からのリカバリ計画を立てる
- コンピュータ利用手続きを確立する
- プログラムの所有権を明確にする
- 従業員と経営者の責任の明確化

- 指揮系統の明確化
- 人物の背後関係の調査

11. 技術的な保護策

技術的な保護策は以下の方法である。

- コスト面での効果
- 自動化
- Override
- 簡潔な設計と操作
- 特権を極力少なくする
- わな
- 管理と利用の独立
- 一般的アプリケーション
- 区分化と保護のレベル
- 分離化，共通なメカニズムを極力少なくする
- 完全さと首尾一貫性
- 道具
- 人間的な面での寛容さ
- 維持
- 監査
- 責任

12. 将来のネットワーク・システム

最後に究極的なシステムとして，カリフォルニア大学バークレー校のDavid Chaum の博士論文で，図19のようなコンセプトがある。

このシステムでは，パブリック・キーとシークレット・キーを別々に持つ事により，お互いの情報を保護するものである。公開鍵暗号方式と言われている。

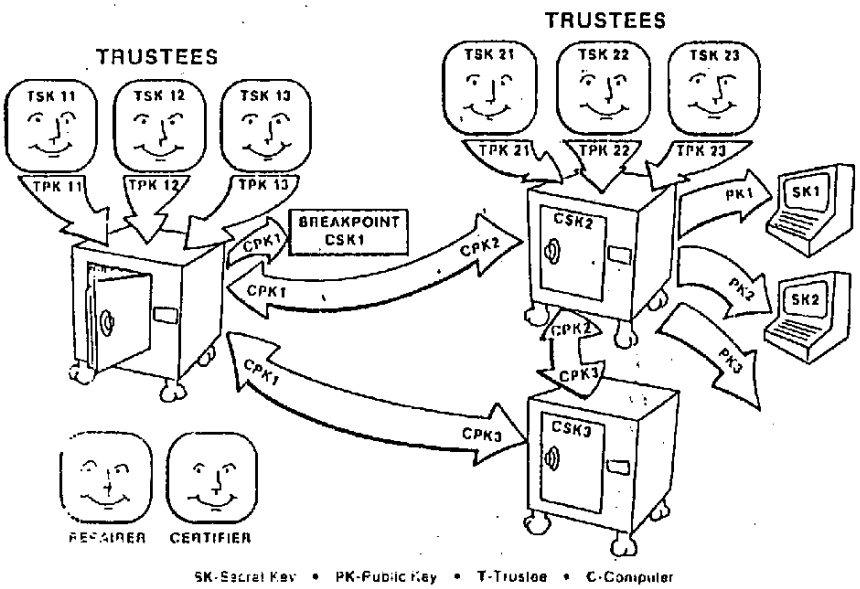


図 19　FUTURE COMPUTER NETWORK TRUSTED by MUTUALLY SUSPICIOUS GROUPS

13. むすび

次の事項を忘れないようにすることが必要である。

(1) セキュリティは人間の問題である。

(2) コンピュータは技術的には完全ではない。

(3) セキュリティには次の２つの扱いがある。

- 事故的なものに対するセキュリティ
- 意図的な犯罪に対するセキュリティ

(4) 問題とするのは情報のセキュリティであり，コンピュータについてのセキュリティではない。

(5) チェックリストに気をつけよ。

(6) 敵のルールで戦わなければならない。

(7) マジノライン・シンドローム。

(8) Nonshareable の問題は機会ではなく悪事を行う者におこなわさせる。

(9) 過去を顧みない者に顧みさせる。

(10) セキュリティは人間の信頼の問題であり，技術的な安全対策は信頼性を上げるものである。

VI EDP Audit Controls

1. 会社概要

- 設立　1976年
- 主要業務
  - リスク・アナリシス
  - コンピュータ・セキュリティ
  - フィジカル・セキュリティ
  - コンピュータ・プライバシー
  - システム監査…総合監査

    ソフトウェア・インテグリティ監査

    システム開発監査

    ミニ（コン）監査

当初は，国防総省やエネルギー省の仕事が中心であったが，今日では民間企業の仕事も受託している。

- 従業員数

  現在20名　内訳：システム監査人5名

  コンピュータ専門家15名

近々に40名にすることが決っているが，監査人とコンピュータ専門家の比率は今後とも守っていく。

- 同業他社

  全米に6社

- 売上高
  - 1976年　10万ドル
  - 1982年 400万ドル

- 社長略歴

社長のロバート・アボット氏は，1971年から1976年まで，国防総省でリサーチプロジェクトを担当し，コンピュータ・セキュリティ関連の業務に従事していた。

2. 業務の主要内容

(1) リスク・アナリシス

リスク・アナリシスを実施し，各種アドバイスを行なう。

(2) コンピュータ・セキュリティのレビュー

(3) ソフトウェア・インテグリティのレビュー

インテグリティは，次の3つに分類される。

① Correct （正確さ）

② Robust （健全さ。適正なトランザクション以外は受けつけないようなシステムを内蔵すること）

③ Trust worthy（信頼性。毎日同じように作動すること）

(4) ソフトウェアの確認および検証

(5) ソフトウェアの保証

- 個人のプライバシー……病歴など
- 自動意思決定…在庫管理など

ソフトウェアの保証は，政府で必要とされているもので，民間企業には要求されていない。しかし，当社としては，民間企業にもサービスしている。たとえば，アメリカ銀行，シティバンク，モービル石油などにこの業務をサービスした実績をもっている。

3. リスク・アナリシス

(1) 資産の確認

(2) 脆弱性の脅威の評価

火災，水害，泥棒，サボタージュ，テロなど

(3) 代表的なセーフガードの評価

煙感知器，扉鍵など

予期される年間損失額の計算

火災，地震などの発生頻度を考慮して，1年間の損失額を予測する

〔例〕 計算は各種条件により異る。

・火災：ホテルなどでは，ハシゴ車の関係で8階以上と以下では数値が異る。

・地震：日本とアメリカでは異るし，地域によっても異る。

(4) その他のセーフガードについての助言

(5) コスト／便益分析

- 可能性と損失を対比して，費用を少くすることも目的である。
- 政府予算では，コンピュータ・セキュリティについてかなり組み込まれている。
- 英国のロイドなどでも，保険についてコンピュータ施設に対する損失の項目がある。

リスク・アナシスは，最近では民間企業でもかなり行なわれるようになってきている。7～8年前までは問題もなく，系統だって実施されるということはなかった。

4. コンピュータ・セキュリティのレビュー

(1) 内部統制

データ処理施設に関しての内部コントロール。

(2) 物理的／管理的セキュリティ

ポリシー，手続き，業務など，具体的なものまで全てを含む。

(3) データ・インテグリティ

(4) ソフトウェア・インテグリティ

(5) データ通信管理

データを受渡しする時，異ったデータに化けることが絶対に起こらないようにするのが大きな目的である。

(6) スタッフの資格と訓練

一度もセキュリティの訓練を受けたことがない人をコンピュータ室に入れたり，オペレーションさせたりすることは危険である。

(7) インタラクティブ・コントロール

(8) 処理後の管理

以上，(1)～(8)までを総合してレビューすることが必要である。このためには，監査とコンピュータの双方の専門家が必要であり，双方の能力をもたなければならない。

コンピュータ・セキュリティを強化するためには，上記(1)～(8)を均等に実施することが必要である。1つだけを強化しても意味がなく，また1つだけ欠落しても意味がなくなる。バランスをもたせることが重要であることを理解する必要がある。セキュリティをさらに一歩前進させるためには，バランスをとり，統一して総合的に前へ進むことが必要である。

5. ソフトウェア保証

この方法を実行しているのは当社が唯一の会社である。

(1) ソースコードのレビュー

ＯＳおよびアプリケーション・システム

(2) ソースコードのコンピュータ可読化

(3) 人間の可読化

(4) マニュアル

ＯＳの場合，非常に細かい説明書が必要になり，マニュアルに従って適正に実施することが必要である。

・会社に適用されるようなソフトウェアを使って実施する。

・主目的は，潜在的な部分を確認することである。

・アルゴリズムの一つ一つは，それ程重要ではないが，まとまると非常に重要になる。

・正しく使われた沢山のアイテムがあり，そのアイテムが100よりも大きい場合は数値的に使用が正しくないことの証明になる。

・単純なアルゴリズムであるが，人を管理する場合，非常に役に立っている。

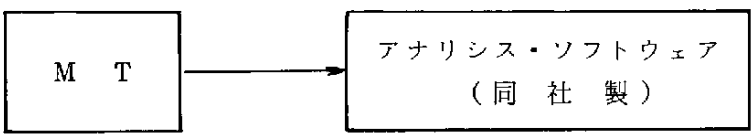
※アナリシス・ソフトウェアの使用：

・モジュールの複雑さをもっとも簡単に指摘する方法により，どこが最も複雑であるかを判断する。

・複雑性係数により上位5つを見るよう指示し，システムの複雑な所をピックアップする。

・システム自体のどこに弱さがあるかも発見出来る。

〔アナリシス・ソフトウェア〕



6. むすび

アボット氏によれば，アメリカのセキュリティ産業は急激に成長しており，今後5年間の成長を次のように予測している。

1981年　　1億5千万ドル（ 375億円）

1986年　　50億ドル（ 1兆2,500億円）

これらは，コンピュータ・セキュリティに関するものを全て含んだ金額であるが，約50%はリスク・アナリシスが占めている。

Ⅶ　TIMNET

1. 会社概要

TYMNET社は，TYMSHARE社から1976年に独立した完全子会社である。組織図は図20に示すとおり。

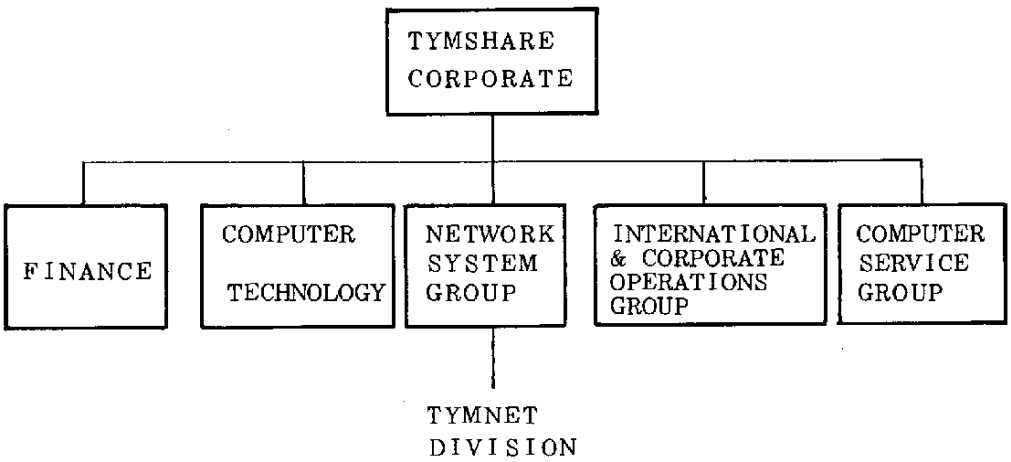


図20　TYMSHARE社の組織図

○ INTERNATIONAL & CORPORATE OPERATIONS GROUP

① TYMSHARE INTERNATIONAL DIVISION

国際タイムシェア　（日　本）

TAYLORIX　（西ドイツ）

ユニリーバ　（イギリス）

CEGIタイムシェア（フランス）　etc.

② DATA NETWORK DIVISION

③ TYMSHARE TRANSACTION DIVISION

④ TELECHECK DIVISION

2. TYMNET

(1) TYMNETは世界で一番大きなネットワークである。

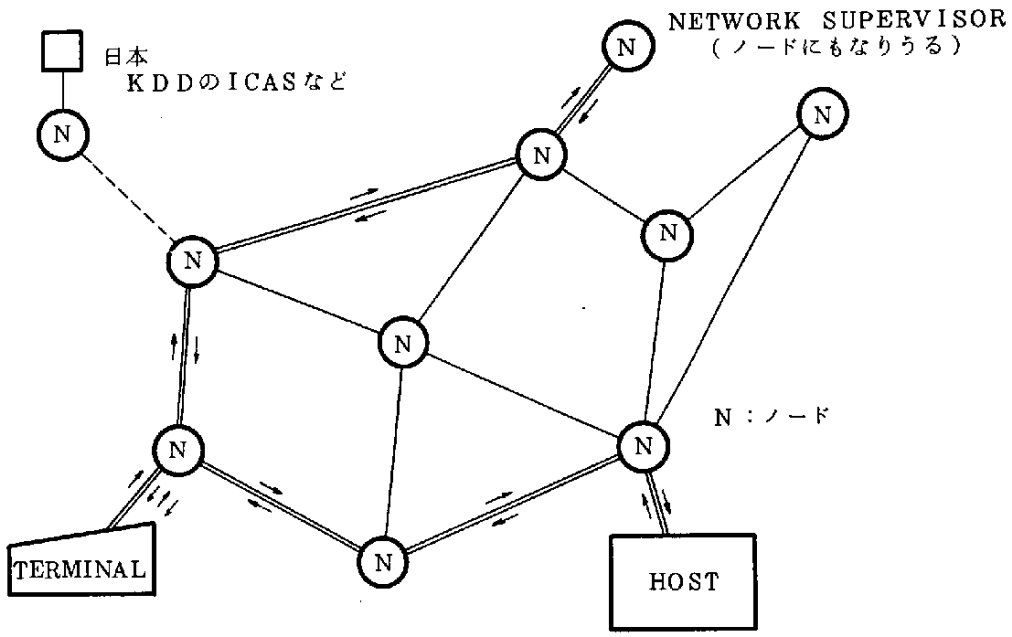


図 21

(2) 他のNETWORKと違うのは思想の違いである。 TYMNET は利益を追求しているのに対し，他社のNETWORK は学術的である。

(3) NETWORK SUPERVISOR

① LOGIN情報のチェックおよび管理

TYMNET の利用開始に先立ち，端末ユーザは，自分のユーザＩＤ，パスワードを入力する必要がある。これらの情報はNETWORK SUPERVISOR へ送られチェックされる。

② 会計情報の確保

ユーザが伝送したデータ量，コネクション・タイム等をNETWORK SUPERVISOR のデータベースへ記録する。

③ 回線の監視

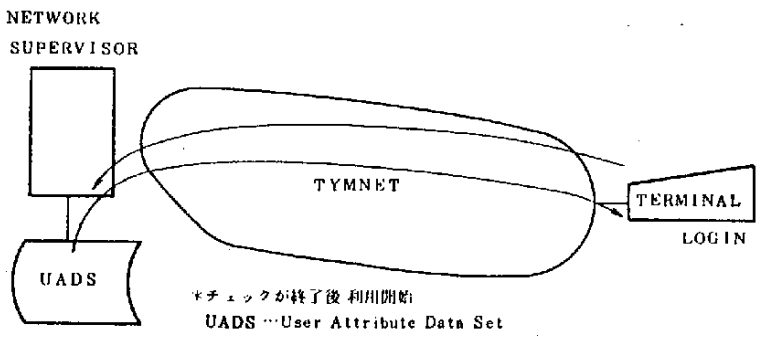


図 22

通信回線の状況を監視する。すなわち伝送エラーがどの程度発生しているか等について記録する。

④ ノードの監視

ネットワーク全体の構成とデータの流れを常に監視している。これによりネットワーク全体としてのスループットを向上させる。

⑤ NETWORK SUPEVISOR 間の監視

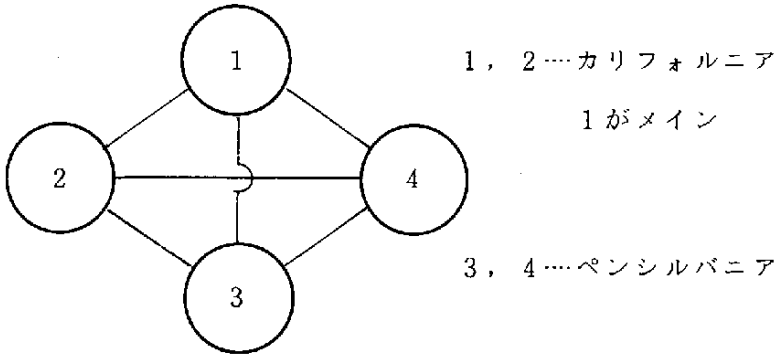


図 23

上図のように，NETWORK SUPERVISOR は 4 台用意されており，通常 1 台が稼動している。これらの 4 台は相互に監視しており，1 台に障害が発生すると自動的にバックアップされる。これら 4 台はチャネル結合されて

おり，相互でポーリングが行なわれていると考えられる。

(4) TYMNET BACKGROUND

① 世界最大のネットワーク

- 1,000 ノード（ほとんどは米国内）
- 350 ホスト
- 4,000 ユーザ
- 延NETWORK 距離 400,000 マイル（64万キロ）

② 歴 史

1972年 サービス開始

1974年 30 ユーザ

1976年 FIELD AS COMMON CARRIER（電話通信業者）
年間 50 %ずつ顧客が増大

1982年 INTERNATIONAL COMMON CARRIER として登録された。

③ 業 務

- TIME SHARING
- BANKING／SAVING DATA SYSTEMS
- CREDIT VERIFICATION／EFT
- MEDICAL DATA SYSTEMS
- COMPUTER TAX PREPARATION
- RESERVATION SYSTEMS
- TERMINAL EQUIPMENT SALES
- NETWORK PRODUCTS & SERVICES

④ 81年度売上 2億5千万ドル

(5) TYMNET VALUE ADDED NETWORK FEATURES

（ＶＡＮ…付加価値データ伝送）

TYMNET におけるＶＡＮの特徴は次の通りである。

① USER ACCESS TO MULTIPLE HOST COMPUTERS

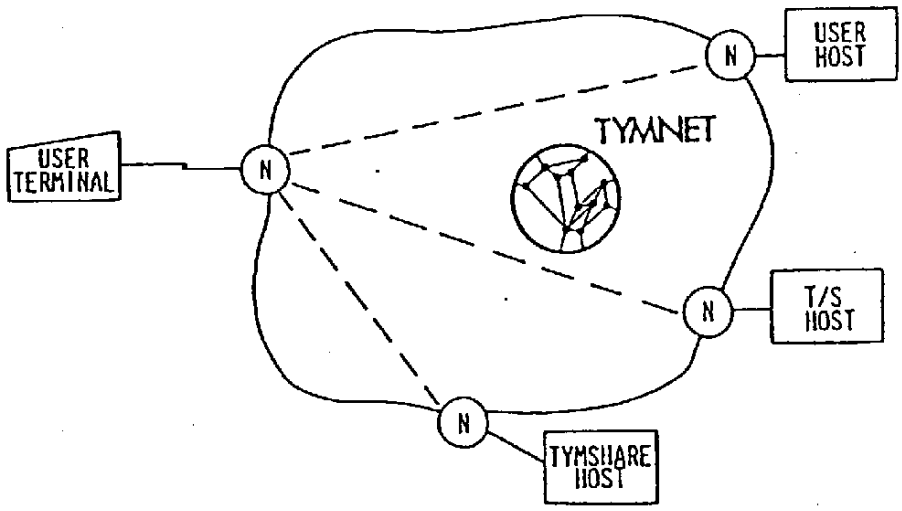


図24

ミニコンピュータによるMulti-Function Node を活用し，各種の端末ホストコンピュータと接続できる。

② GATEWAYS TO INTERCONNECT PUBLIC & PRIVATE NETWORKS

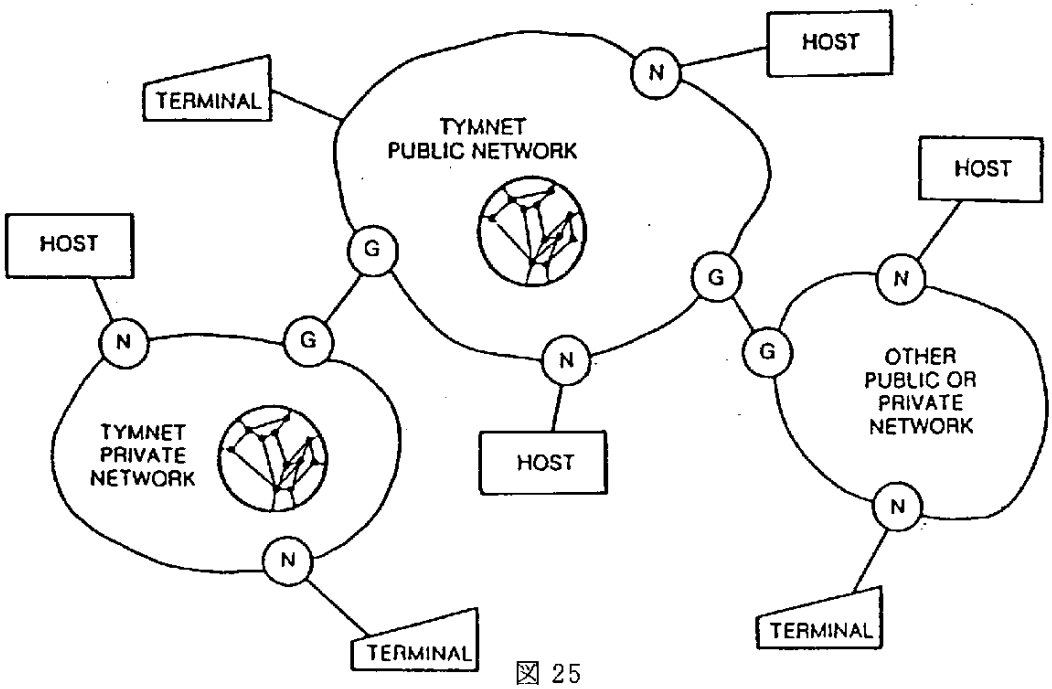


図 25

TYMNET とコネクトしている主要ネットワーク

- VENUS　（日　本）
- DATRE-P　（西ドイツ）
- IPSS　（イギリス）
- TRANSPACK（フランス）
- DATAPACK　（カナダ）
- RADIOスイス（スイス）
- ITC　（イタリア）

③ ROUTING TO AVOID CONGESTION & OUTAGES

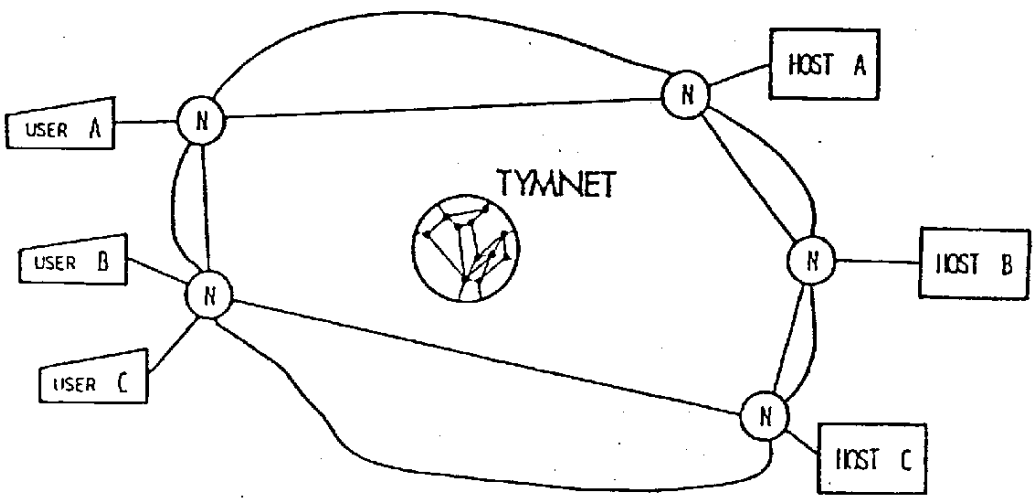


図 26

ネットワーク・データ・サーキットの共用により，ネットワーク負荷の分散，代替パスの利用による遅延が回避できる。

④ SHARED USE OF NETWORK DATA CIRCUITS

1パケットに複数ユーザを収容し伝送を行ない，データの合成，分割はノードで行ない，伝送効率を向上させる。

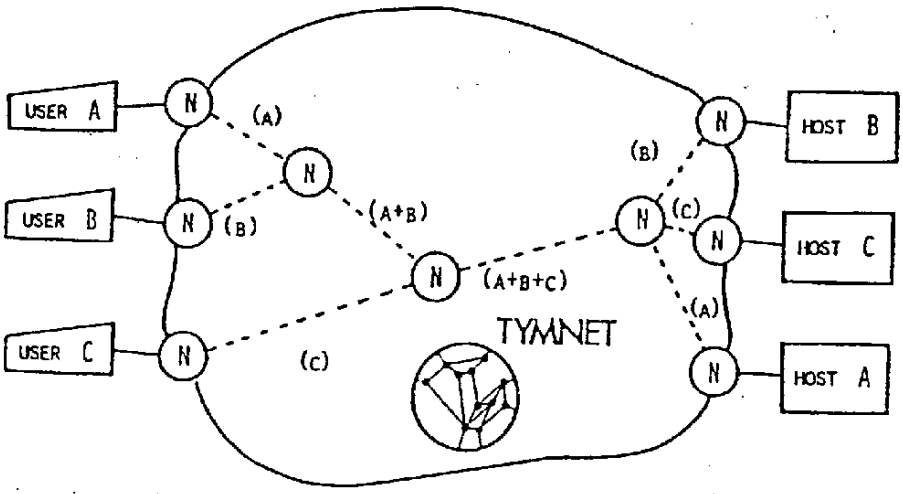


図 27

⑤ MULTI-FUNCTION NODE PROCESSORS (TYMNET ENGINES)

TYMNETには，自社開発のTYMNET ENGINE（32ビットのミニコン）をNODEおよびNETWORK SUPERVISORに使用している。

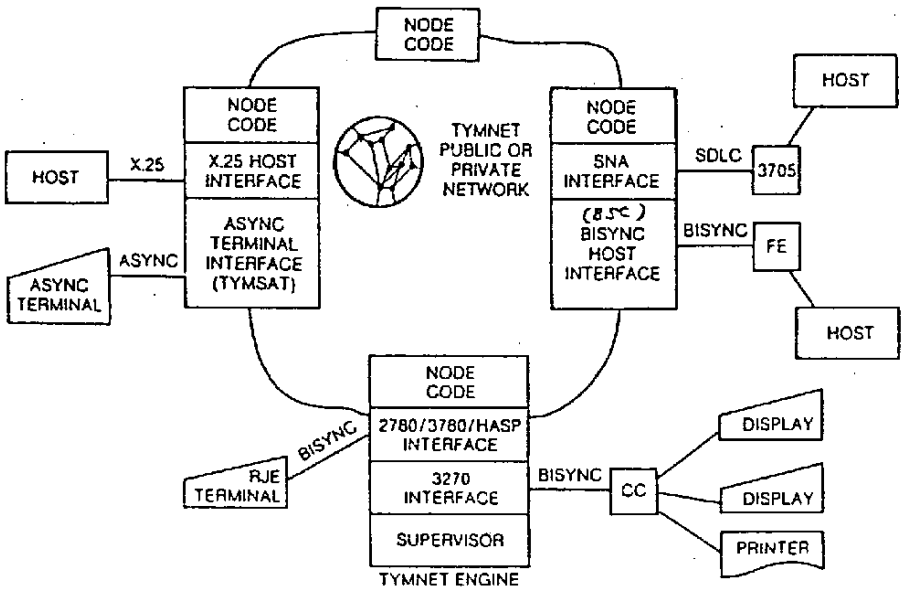


図 28

⑥ MESSAGE SWITCHING

(ON TYME-Ⅱ ERECTRONIC MAIL SYSTEM)

TYMNET 社のサービスは，ON TIME Ⅱ というエレクトロニック・メールがある。これは，メッセージの発信・受信機能のみではなく，メッセージの編集機能，ファイリング機能などがあり，ワードプロセッサとメッセージ交換の機能を兼ねそえている。

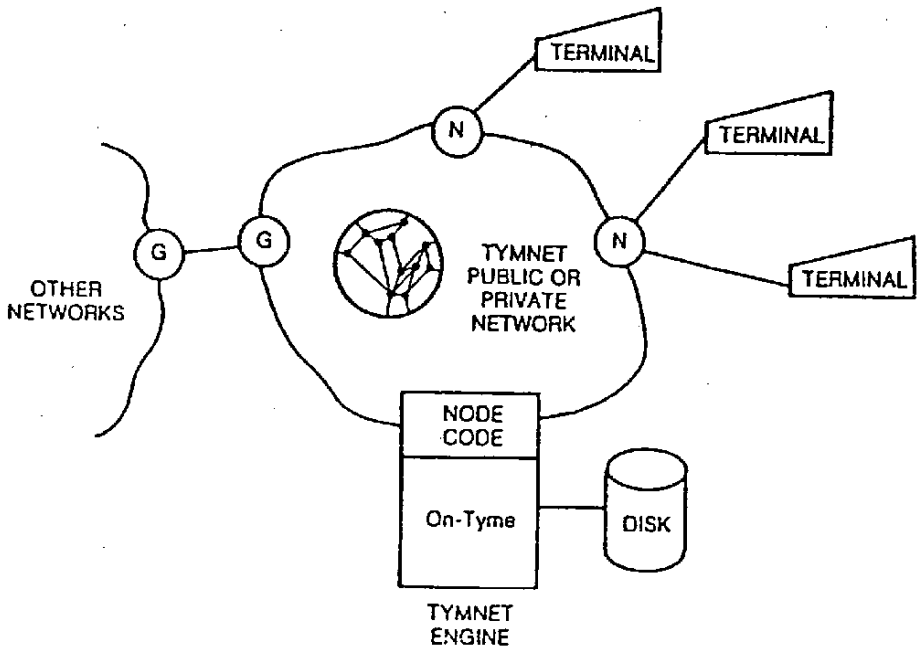


図 29

(6) TYMNET ENGINE

① TYMNET の NODE に当るミニコンピュータは TYMNET Ⅱ ENGINE と呼ばれ高度な機能を持った INTERFACE MESSAGE PROCESSOR である。

② NETWORK SUPERVISOR も当然この TYMNET Ⅱ ENGINE が使用されている。

③ 性 能

32 ビットプロセッサー

256 汎用レジスター

メインメモリー１MB以上

メモリーサイクルタイム　750ns

マイクロサイクルタイム　125ns

④　HARDWARE DESIGN FOR RELIABILITY

SPECIAL POWER SUPPLY & CHASSIS

EXTENSIVE MICROCODE & HARDWARE DIAGNOSTICS

⑤　SPECIAL OPERATIONAL FEATURES

REMOTE LOADING

POWERFUL FRONT PANEL

SUPER CLOCK

(7)　ISIS

①　TYMNET の通信制御用のソフトウェアはISIS（INTERNALLY SWITCHED INTERFACE SYSTEM）と呼ばれており，CCITT のX25，X75，X3，X28，X29 をサポートし，海外ネットワークとの接続をも可能としている。

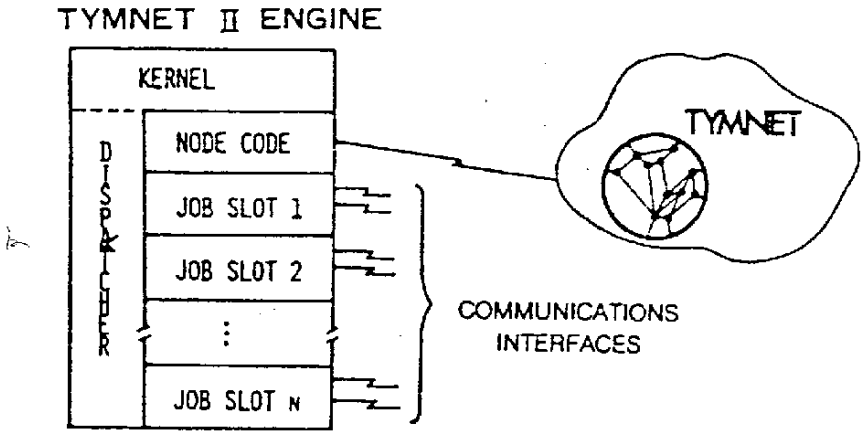


図30

KERNELと呼ばれるオペレーティング・システムとプロトコル・コンバージョン用の各種アプリケーションから構成され，JOB SLOTがインタフェー

スをとりTYMNET ENGINE 当り最大16 SLOTまで動作可能である。

② 海外ネットワークとの接続はCCITT 標準プロトコルを用いて接続することが可能である。

③ CCITT 標準プロトコル

ⓐ X 25

DATAPAC （カナダ）

TELENET （アメリカ）

BPO／IPSS（イギリス）

TRANSPAC（フランス）

TANDEM

PRIME

COMM-PRO 3705

MEMOTEC

SYSTAR

ASSOCIATED COMPUTER CONSULTANTS

CAMBRIDGE TELECOMMUNICATIONS

DATA GENERAL

DARTMOUTH TIME SHARING SYSTEMS

NCR COMTEN

ⓑ X 75

TRANSPAC（フランス）

KDD／VENUS（日 本）

ⓒ X 3，X 28，X 29 COMPATIBILITY

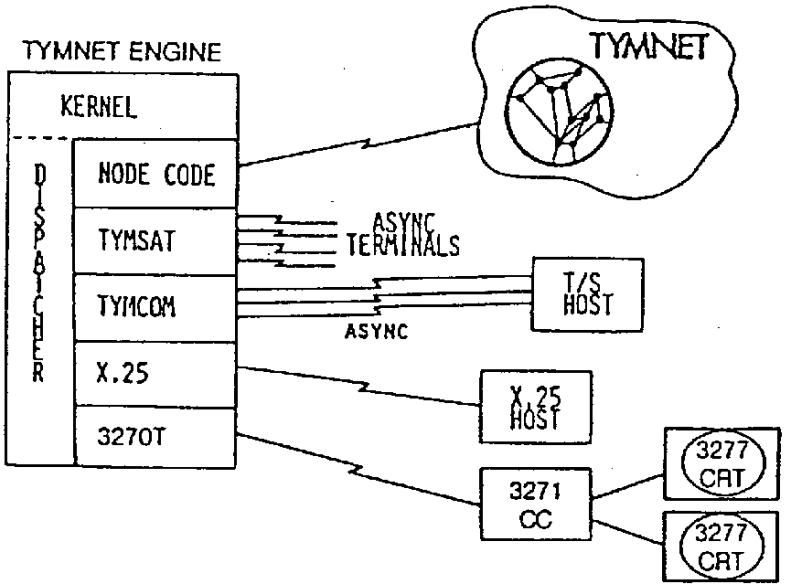


図31. TYPICAL ISIS NODE

・NODE CODE ……ノード間プロトコル・ソフトウェア

・TYMSAT ……TTY端末のHOSTインタフェース用ソフト

・TYMCOM …… 〃 ターミナル・インタフェース用ソフト

・3270T ……3270のターミナル・インタフェース用ソフト

これ以外にも 2780／3780，3270H 等がある。

(8) TYMNET NETWORK INTERFACES

① HOST INTERFACES

X 25 SNA BISYNC(BSC) ASYNC

② HOST PROCESSORS SUPPORTED

AMDAHL

BASIC TIMESHARING

BURROUGHS

COMPUTER AUTOMATION

CONTROL DATA

DATA GENERAL

DATAPOINT

DEC

HEWLETT-PACKARD

HONEYWELL

IBM

NATIONAL SEMICONDUCTOR

NCR

PRIME

UNIVAC

XDS

③ TERMINAL INTERFACES

ASYNC (TO 9,600 Bps)

BISYNC 3270 (TO 9,600 Bps)

BISYNC 2780／3780／HASP (TO 9,600 Bps)

X 25 (TO 56,000 Bps)

SNA (TO 56,000 Bps)

TINET (TO 1,200 Bps)

(9) セキュリティに関して

① パスワード(ノンプリンティング)

NETWORK SUPERVISORにSTOREチェック

② インターライン・プロトコル

情報を解析できない

・SHARED PACKET

・LINE ……NON ASCII

・RANDOM ROUTINE

サリバン氏は，大したセキュリティではないが，現在のところ支障は来たしていないと語っている。

Ⅷ　S D C

1. 会社概要

ＳＤＣ（システム・ディベロプメント・コーポレーション）は，情報技術とシステム・サイエンスに関する専門会社として，世界で最も大きく，また豊かな経験を持つ会社の１つである。

４分の１世紀にわたり，ＳＤＣは，政府機関，教育関係，医療保健，エネルギーおよび環境関連産業，その他多種多様な商工業関係企業に，技術的な支援とシステムのサービスを提供してきている。

●沿　革

1955年　ランド・コーポレーションの１事業所として誕生。

1956年　非営利団体の政府関係事業として独立。

1969年　営利企業として事業開始。

1981年　バロース・コーポレーションの子会社となる。

●事業内容

コンピュータを中心とした

システムの分析

システムの設計

システムの開発

システムの構築

システムの運用

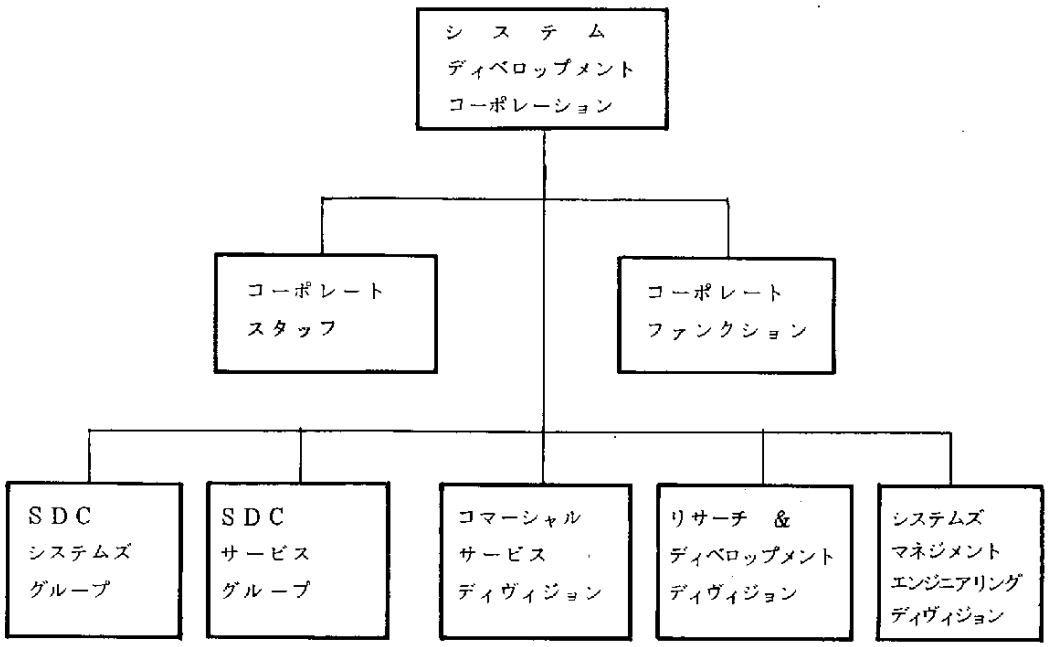


図 32　SDCの組織

2. 部門の業務内容

(1) SDCシステムズ・グループ

SDCの中での最大のグループであり，大規模な情報システムの構築に関して，

○プライム・システムズ・コンストラクタ

○システム・エンジニア・インテグレータ

○ソフトウェア・システム・ディベロッパ

○ヒューマン・リソース・エンジニア

の役割を果している。

アプリケーションの内容としては，

○コマンド・コントロール

○宇宙開発

○人間系システム（教育と評価）

○工業技術とその高度化プログラム

○システムとソフトウェアのエンジニアリング

○気象観測の画像処理

○経営情報システム，など

がある。

主たる顧客としては，

○アメリカ空軍

○アメリカ海兵隊

○アメリカ海軍

○アメリカ農林省

○アメリカ国防総省

○アルゼンチン

○インド

○日　本

○ＮＡＴＯ

○ロスアンゼルス警察，など

殆んどが政府関係であるが，ＳＤＣの一番の売り物は人間である。

(2)　ＳＤＣサービス・グループ

オペレーションの担当部門であり，

○トータル・ファシリティ・マネジメント

○ソフトウェア・サービス

○トランザクション・サービス

○コンピュータ・オペレーション，など

を行なっている。

アプリケーションの内容としては，

○教育関係のアプリケーション

○医療事業

○エンジニアリングとテクニカルのサポートサービス

○福祉関係事業

○自動フード・スタンプ関係

○ファシリティ・マネジメント

○ユニバーサリィ・コントロール・システム

○プログラミング

などを上げることができる。

主たる顧客としては，

○アメリカ文部省

○アメリカ運輸省

○環境保護協会

○交通安全協会

○ＮＡＳＡ

○ニューヨーク州

○オハイオ州

○フロリダ州

○ニューヨーク市

○ボストン大学

○バンアメリカン保険会社

など，国関係が少なく州又は地方行政府関係が多い。

(3) コマーシャル・サービス・ディヴィジョン

広範囲な地域にサービスを供給する組織で，その内容は，

○ＳＤＣ・サーチ・サービス

○クレーム・アドミニストレーション・サービス

○コンピュータ・サービス

○データ・サービス

などがあり，サービスの範囲も

○ロスアンゼルス

○東京

○ロンドン

○デトロイト

と広範囲である。

主たる顧客は，ビジネス関係が中心であり，

○ゼネラル・ビジネス

○保険

○医療

○エネルギー

○ファイナンス

○輸送関係

と，多岐にわたっている。

(4) リサーチ＆ディベロップメント・ディヴィジョン

ＳＤＣの将来のビジネスに必要な技術の研究開発を行なっている。

その内容としては，

○コンピュータ・ネットワーク

○分散処理

○システム・セキュリティ

○ユーザ・インタフェース

○基礎学問的なシステム

などがある。

研究開発事業は，自己資金によるものと政府資金によるものの２通りの方法があるが，アメリカ国内では，一番のリーダー格である。

特に，システムのセキュリティに関しては，政府・民間を通じて一番進んでいると自負している。

新らしい技術として紹介できるものに，SLANTがある。

これは数マイル間の限定された地域のネットワークにおける情報交換のデータ保護のシステムであり，

- ユーザ・ワークステーション
- 複数の独立したホスト・コンピュータ
- 相互に連携された限定地域のネットワーク
- アメリカ国防省基準のプロトコール
- 分散型データベース
- ネットワーク・セキュリティ

のそれぞれをテーマとしてかかえている。

(5) システム・マネジメント・アンド・エンジニアリング・ディヴィジョン

エネルギーに関する事業が主であり，

- システム・エンジニアリング
- プロジェクト・マネジメント
- プロジェクト・プランニング・コントロール
- エンジニアリング・アナリシス（STARDYNE）
- デザインの再確認
- 建設の施工管理
- 調達
- 品質保証
- スペシャル・スタディ
- プロジェクトの採算分析

などを行なっている。

主たるプロジェクトとしては，

- ガスの遠心分離機による濃厚化プラント
- アラスカの天然ガス輸送システム
- 自動車燃料のアルコール利用プロジェクト

○核燃料の緊急状態感応設備プラント

○公共事業

○STARDYNE

などを上げることができる。

これらエネルギー関係の事業は，スリーマイル島の事故以来特に力を入れている。

（㈱　STARDYNEとは構造物の技術的解析用のパッケージであり，構造物がどのような組立てであれば一番よいかを解析する。）

主たる顧客は

○エネルギー省

○運輸省

○ネブラスカ・アルコール燃料コーポレーション

○ロスアンゼルス水道電力局

○アトランティック・リッチフィールド・カンパニー

○南カルフォルニア・エディソン

○グッドイヤー・アトミック・コーポレーション

などである。

(6)　その他

①　ＳＤＣの人員構成

●専門の特技者

ソフトウェア技術者	43％
システムアナリスト	22％
その他の専門職	18％
科学技術者	14％
ヒューマンファクターズ	3％

●専門の学位者

学　士	63％

修　士　　31％

博　士　　6％

●専攻別の学位者

数学　　22％

管理科学　　18％

工学　　17％

人文学　　15％

人間科学　　11％

自然科学　　9％

コンピュータ科学　8％

② ＳＤＣの業績

●売上げ（単位：百万ドル）

1981年　223.5

1980年　186.8

1979年　163.1

1978年　159.4

1977年　136.6

●税引前利益（単位：百万ドル）

1981年　19.6

1980年　14.1

1979年　9.7

1978年　5.2

1977年　5.6

●純利益（単位：百万ドル）

1981年　11.0

1980年　7.7

1979年　6.2

1978年　　2.0

1977年　　2.6

1982年　　18.0（予想）

● 受注残（単位：百万ドル）

ファーム関係

1981年　271.7

1980年　190.1

1979年　226.3

1978年　142.8

1977年　125.7

ソフト関係

1981年　581.3

1980年　80.5

1979年　58.6

1978年　53.4

1977年　59.6

特にソフト関係の受注残は，今後ますます続くことが予想される。

● ＳＤＣの1981年における売上げ

国防総省　　39％

その他の連邦政府　　26％

（殆んどは，ＮＡＳＡ関係）

州及び地方行政府　　11％

外国関係　　5％

（外国関係の比率は低いが，現在非常に伸びている。）

コマーシャル　　19％

● 軍関係の1981年における売上げ

空　軍　　39％

（殆んど衛星関係）

陸　軍	14％
海　軍	38％
その他	9％

その他ＳＤＣは，約4,000人の従業員をかかえ，サンタモニカに本社をおき，全米各地に支店を持っている。

また，外国に関しては，カナダ・フランス・日本をはじめ，約57カ国の国々と取引の実績がある。

付属資料
コントロール・ガイドライン

付属資料

コントロール・ガイドライン

将来のコンピュータ・システム開発および利用のために

原題：Control Guidelines
… for use in the development and implementation
of future computerized systems

マサチュセッツ生命保険会社
監査部ＥＤＰ監査グループ　1977年1月発行

コントロール・ガイドライン

本文書起草の目的は，将来の標準化に備えてシステムズ・コントロールやコントロール手続きのガイドラインを設定することである。このガイドラインにそって，先々システムズ・コントロールは総合監査部の手で実施されよう。個別的にせよ，あるいは組合せにせよ，これらのコントロールが実施の運びとなれば，実際的な運用ベースにおける最良のシステム・セキュリティが確保できるに違いない。

コントロールの定義

「コントロール」とは，コンピュータ・システム内部の一貫性と正確さに一定の基準を与える手段である。これは，つぎのような機能をもつ。

- ○企業資産のセーフガード
- ○会計データの正確さおよび信頼性の検証
- ○運用効率の促進
- ○経営政策との密着性を確保
- ○監査証跡の提供

コントロールの設計はアプリケーションにより異なるが，その基本的な目的および必要性は一定不変のものである。

資産および負債の金額を正確に把握することは，全てのコントロール手続きでは第一義に属することであり，コントロールは常に財務報告や総勘定元帳の収支およびこうした収支残高を示す数字に関係した金額取扱欄に置かれねばならない。

コントロールの設定コストとコントロールなしですますコスト／リスクのバランスは，コントロール設計・評価においてシステム設計者が絶えず考慮せねばならないテーマである。また時間，材料，資産等の損失リスク，ユーザおよび保険契約者の満足，経営者の信用等も，コントロールを開発・利用する際必要な時間

や素材を考える時，コントロール・コストの対として重視される必要がある。もしこの間に適切なバランスがなければ，そのコントロールは，当初の意図を超すか，あるいは及ばないという結果になる。

フォーマット

このガイドラインの論理的立場を強化するため，コントロールの発想概念は，12の主要なカテゴリに分けられた。また各カテゴリは，ＩＳＤやユーザ分野の責任により，さらに細分化されている。大抵の場合，コンピュータ・システムに関連しユーザ利用に向けたコントロールの設計や提供は，ＩＳＤの責任に入る。

① 入力コントロール
② 処理コントロール
③ 出力コントロール
④ 直接更新手法を使用するシステムのコントロール
⑤ データ保存
⑥ エラー・コントロール
⑦ データ変更コントロール
⑧ ファイル・セキュリティ
⑨ プログラム／システム・ドキュメンテーション
⑩ プログラム変更コントロール
⑪ 責任の分担
⑫ マネジメント・トレイル

論理的解釈の立場を一層明快にするため，12の主要カテゴリは，各々対応するコントロール・タイプに分化された。

① 手続きコントロール ― データ準備，受領，処理，蓄積，出力などのためのコントロールは，データの正確さ，一貫性，継続性を保つものである。
② 管理的コントロール ― このコントロールは，システム・プログラムの正確さと継続性を保証するため設計される。
③ 組織的コントロール ― 責任の存する正当かつ適切な部位を確かならしめる

意図をもったコントロール。

内容目次

Ⅰ．手続きコントロール

A．入力コントロール

ISD（Information Systems Department）の責任

1. 転送フォーム(注1)は，データが不正確あるいは不完全に記録される機会を最小限

に抑えるよう設計されなければならない。

2. 機械読取可能なフォームへのデータ変換（カード入力，直接エントリ）は，間違った変換により発生するエラーを極力抑えるようにコントロールされなければならない。

a．データ検査

b．ユーザまたはコントロール・グループによる検討，あるいはトランザクションの調節制御

3. バッチの場合，ＩＳＤはバッチ・コントロール記録からのコントロールおよびハッシュ・トータルが入力から取られたトータルに対し検査されるよう保障すべきである。

4. バッチにおけるエラー量やユーザの訂正速度にもよるが，全てのエントリが編集された後，全バッチを除去することが望ましい。

5. エラーは，修正や再付託のためユーザ分野別のエラー・リストにのせるべきである（「エラー・コントロール」の項参照）。

6. データが磁気ファイルから入れられつつある時，ファイルのラベルは，システム・ソフトウェア（例えばＴＭＳ）や正しいファイルがランされ得る他の何らかの手段によって検証されるべきである。

a．正しい日付け

b．正しいサイクル

c．正しいファイル／バッチ・ナンバ

d．正しいファイル識別子

7. オンラインまたはリアルタイムのシステムを使用する場合，コントロールはつぎのような内容を確実にしなければならない。

a．端末が有効な伝送装置である。

b．ユーザは，アクセスする合法性と権限を有する。

c．いかなるメッセージも失なわれない。

1）メッセージ・カウント

2) メッセージ再生

3) エゴー・チェック

d. メッセージが有効である（これは通常の入力コントロール，編集ルーチン等により実行できる）。

e. ログ（トランザクション・コントロール・ログ）に記載される問合せ，更新等はつぎの事柄を忘れてはならない。

1) 誰がどのターミナルから

2) 時刻と日付け

3) 行われたトランザクションまたはオペレーション

4) 影響をうけたファイル

8. 入力コントロールのタイプはつぎの通りである。(注2)

a. トランザクション・カウント

b. データ予測

c. キーパンチによる，またはキーパンチとは別なカード検査

d. 機械読取可能ドキュメント入力

e. 分離入力妥当性検査ラン

f. 入出力コントロール・グループ

g. 入力データセットのチェック

h. 入力妥当性検査

（注1）：転送ドキュメントは，このガイドラインにあっては，ソース・ドキュメントからデータを利用するユーザにより用意されるフォームと定義される。またソース・ドキュメントは，データが取られたオリジナル文書として定義される。

（注2）：付録Bの「コントロール説明およびその実例」を参照。

ユーザの責任

1. トランザクションの適当な許可，開始，点検の責任は，つぎの方法により明確にされるべきである。

a．責任の明確化

b．高度な責任レベルを確保するための許可業務の点検

c．任務の分割

1）記録保管

2）資産保護

3）検討／許可

2. 転送書類は，その作成，点検，許可の責任について，フォーム上の識別コード，あるいは作成者，点検者，許可者のイニシャルを当該書類上に記入させることによって責任の所在を明らかにしなければならない。

3. 最近のドキュメントを識別・チェックできるよう文書に日付けを添付する。

4. トランザクションが膨大であったり，異常または稀にしか現れないタイプの場合，転送ドキュメントやそのトランザクション用のログ・エントリに監督者は署名すべきである（この時使用されるのは，トランザクション・コントロール・ログ(注3)である）。

5. 転送フォームの稼動は，作成とシステム・エントリのプロセスの間で何も失なわれないようコントロールされねばならない。

a．事前に番号を付与したフォーム — もし可能なら，このフォームの採用により，全転送フォームの算定が可能となり，行方不明のフォームの指摘が容易となる。

b．何が，誰から，誰に転送されているかを示すルート・スリップ。

c．でき得るならば，共通取引グループに区分する。

6. バッチは，つぎの方法でコントロールされる必要がある。

a．コントロール・トータルは，キーとなる識別子や金額の欄か（算定数のハッシュは金額のトータルと同程度に重要），バッチ・レコードの数の上に置かれるべきである。

b．もしバッチ・コントロール・グループがあるなら，それは，全入力を受信し，バッチし，コントロール・トータルを決定し，コントロール・カードを

生成し，バッチをＩＳＤの処理に提供するために用いられるべきである。

c．バッチ・コントロール・グループが存在しないなら，バッチ・コントロール・トータルを算出し，コントロール・カードを作成し，そして作成者はバッチ・コントロール・ログ・エントリを実行しなければならない。その際責任ある監督者は，そのバッチを取りあげ，コントロール・カードを検査し，コントロール・ログ・エントリを検証しサインするとともに，バッチをＩＳＤに提出する必要がある。

d．コントロール記録の共通認識を得るため，汎用的な識別子が用いられなければならない（例，保険証券ナンバ＝9's）。

（注３）：コントロール・ログは本ガイドラインにおいては，ユーザによりシステムに投入されたトランザクション／バッチの統計を内容としてもつ帳簿（あるいは書類，書式）を指している。追跡調査とか参照用に用いられることが主目的となっている。

B．処理コントロール

ＩＳＤの責任

1. 処理コントロールには，つぎの意図がある。

a．システムからの出力＝システムへの入力。

b．プログラム・インタフェースは，送付されたプログラム出力と受け取られたプログラム入力を合致させる必要がある。

c．さらにシステム・インタフェースに要求される役割はつぎの２つである。

1）送付されたシステム出力＝受け取られたシステム入力。

2）共用ファイルは，送受両システムのコントロール要件を満足させなければならない。

2. トランザクション・ソースに密着して開発された平衡コントロールは，出来得る限り実際的な処理を通じて行われるべきである。

3. プロセシングのコントロール手法

a．ランごとにコントロール・トータルを集計する。

1) ハッシュ・トータル

2) 金額コントロール・トータル

3) 記録カウント

b. 極めて重大な異動およびコンピュテーションの結果をチェックする。

1) 限　界

2) 合理性

3) 欄からのはみ出し

4) 内部ファイル・ラベル

4. もし入力がバッチ・フォームで，そのフォームのまま維持できるなら，バッチ・コントロール・トータルは，プロセシングの全体を通して集計されるべきで，詳細な点まで帳尻の合ったものでなければならない。

5. 1つのラン／モジュールや1つのシステム内部でプロセシングがかなり容易に再開できるポイント（例，ジョブ・ステップの間）は，再開部位として「マーク」される必要がある。

6. プロセシングが再開点に達した時，処理中のデータは，指定ファイルに書き込まれなければならず，この情報こそが，失敗以前の最も近い再開点までシステムを再ロードするために用いられる。

7. 全データのバックアップは，「データ保存」の項で示されているレベルまで完全性と十分性を持たなければならない。

ユーザの責任

1. ユーザは，つぎのような作業項目に従い，コントロール・プロセスで進行中の事務管理に関心を払わなければならない。

a. 入力から出力までの取引の定期的追跡またはエラー・リストの作成。不一致は調和解消されなければならない。

b. 出力レポート上のトータルを定期的に手作業により横計算（クロスフット）する。可能ならレポートの品目記載行でも同様の作業を行う。

c. 別個のレポート間で共通するデータに偏差がないようチェックする。

d．機械生成値の定期的な有効性チェック。

2. ユーザ・サイドの点検により生じた処理コントロールに対する彼等の不満は，直ちにＩＳＤに通告される必要がある。

（注）ユーザ・チェックの頻度は，当該システムの複雑さやインパクトの大きさに左右されることが多い。

C．出力コントロール

ＩＳＤの責任

1. 処理および入力のコントロール・トータルは，出力が準備される際，全てのレコードが一時に算定できるよう，出力コントロール・トータルと結果に一致を見なければならない。

2. 出力コントロール・トータルは，出力データセット・ファイルの後書き，およびそれが出力の検査に使用できるあらゆる場所に書き込むべきである。後書きレコードに含まれるものはつぎの通り。

a．識別子（例，保険証書ナンバ＝9's）

b．ファイル／バッチ・ナンバ

c．レコード・カウント

d．重要欄のコントロール・トータル／ハッシュ

3. 出力設計では情報の誤解や誤用を防ぐため，印刷書式を指定すべきである。

a．タイトルは全て，無意味なものであってはならない。

b．作成された全レポートには，処理されたデータ，そのデータの日付け（あるいは処理日時）が記載される必要がある。

c．レポートの各ページに必ずページ・ナンバを入れる。

d．コンピューテーションに含まれる全ての変動要因は，チェックを容易にするためにも印刷されなければならない。

e．プリントアウトの最後は，標準的なメッセージ（例，「レポート末尾」）で表示する。

4. 出力の正確度を高めるため，選択的にシステム・チェックを行う方法もある。

このようなチェックには，つぎのようなものがある。

a．関連欄の横計算（クロスフット）チェック

b．残高（バランス）チェック

c．既定限度との比較

d．サイズ，ブランク，アルファベット，数字等の有効性チェックのための欄内容点検

5. 出力配布先管理リストは，配布が認可先に限定されるよう出力管理要員により保存される必要がある。

6. 出力の配布先と時期を適切にするため，その配布手順を確かなものとする。遅滞が予想される場合，ユーザは早急にその旨通告すべきである。

7. ユーザは，各レポートの必要性が依然継続しているか否か，周期的に自答すべきである。

8. 事前に印刷されたフォームが出力として用いられる時，ナンバリング済みなら管理が事の外容易となる。

9. 出力コントロール・グループは，完全さ，合理性，均整を対象に出力を精査すべきである（必ずしも正確度はこの場合要求されない）。

ユーザの責任

1. ユーザは各レポートに対する必要性を定期的に点検し，不必要なものは中断すべきである。

2. 出力の配布管理リストは，ユーザにより作成維持されなければならない。出力管理要員はこのリストを利用して，配布予定の出力の全部をタイムリに受け取ったかを確認し，当該レポートの配布許可を受けた人物にのみ手渡っているかチェックする。

3. ユーザは，トータルの正確さだけでなく，その品目の合理性についても適宜出力を点検する。

4. 出力結果を入力と比較し，手作業によるコンピュータ処理をチェックするため，個々のドキュメントまたはリストを選択的に点検する方法もある。

5. ユーザは，問題に直面すれば直ちに適当なＩＳＤの接触先に通報すべきである。

6. 微妙なデータに対しては，特別な配布手順を設定する（例えば給与支払データ）。

7. 事前に印刷されたフォームが使用される場合，定期点検を行い廃止フォームの全てを除去破壊する必要がある。

D．直接的更新手法を用いたシステムのコントロール

ＩＳＤの責任

1. システムのアクセスは，認知されたターミナルとオペレータに限られる。

2. アクセス・セキュリティ・マトリクスを使用する際，ファイルに対する行為レベル（例えば，インクワィアリ，更新）は，許可レベルと常に対応しなければならない。

a．必要でかつ適当な場合，この方法は，所定レコードの欄にも選択的に拡大使用することができる。

3. 成功あるいは目的の如何にかかわらず，全てのアクセスはシステムによってログされる必要がある。

4. 一定時間何の活動もおこさなかったアクセスは，全て自動的にシステム側で中断されるべきである。耐え得るレベルとして，われわれは２～３分の非活動時間を勧告する。

5. ファイルの直接的更新は，つぎのような結果をもたらす。

a．レコードが生成されバックアップ・ファイルに追加される。このレコードは，更新対象とされるレコードの前後のピクチャーをも含むべきである。

b．エントリの日付けおよび時刻を伴なったトランザクションと開始者のコードが取引ファイルに投入される。

1）このファイルからトランザクション・ログは，コスト・センタ別にリストされ，点検のためユーザ分野のリーダに定期的に配布される。

c．最後のシステム・バックアップ・ダンプから算出されたコントロール・ト

ータルと，最後のバックアップで生じたプロセシングのためのコントロール・トータルの累計を内包するコントロール・ファイルは，当面する作業のために，これらの累計を更新させなければならない。

d．上述したアプリケーションの理論的システム・ダイアグラムは，図1に示す通りである。

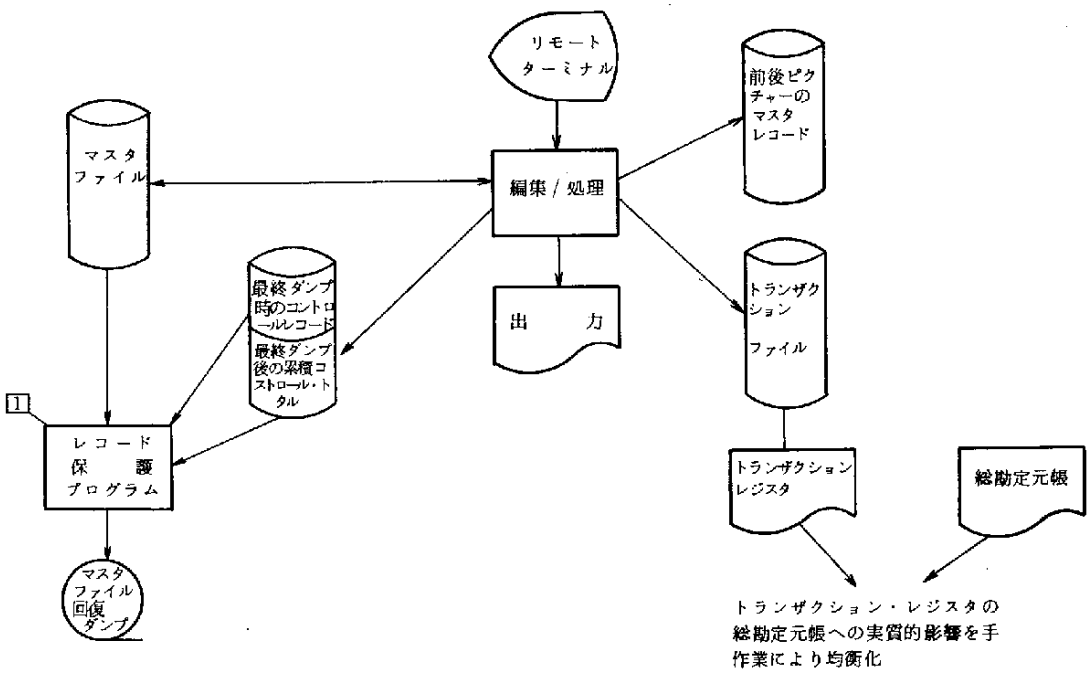


図1. 記録保護プログラムにおいては，古いコントロール記録やコントロール累計は，ダンプ中にマスタ・ファイルから抽出されたトータルと帳尻を合せられる。

ユーザの責任

1. 責任あるユーザの管理者レベルは，ファイルを直接更新する必要があり，かつ，またその能力を有する人のみが行い得ることを保証すべきである。
2. トランザクション・ログ・リストは，責任あるユーザの部門リーダにより徹底的に検査され，異常な，過剰な，不合理な，そして不許可の行為がないかどうかチェックされなければならない。

3. 疑問の残る品目は即座に精査を行い，ファイルのインテグリティに支障がないようにすべきである。

E．データ保存

ＩＳＤの責任

1. データ保存のフォーマットおよびその期間に対する規制機関の要求は，全て満たされるべきである。情報源として，つぎのものがあげられる。

a．適当なユーザ部門

b．レコード・マネジメント・サービス

c．法律担当部門

d．全社的コントローラ部門

2. データは，生産ファイルのバックアップとユーザの担当部門の活動へのサポートのために必要な時間だけは，少くとも保持されなければならない。

ユーザの責任

1. システム設計時にユーザは，システム出力の有効性チェックに必要な時間数をあらゆる努力を払って決定すべきである。この長さがどうであろうと，こうして決定された所要時間は，出力およびその出力の生成に必要なデータにとって最少の保存期間となることが大部分である。

2. ユーザは，その最低保存期間について，ＩＳＤと緊密に連絡をとるべきである。この期間の決定要因はつぎのとおりである。

a．バックアップと調整用に公刊されている洗練された数値。

b．法律。

c．外部調査機関（例，内国歳入庁（ＩＲＳ），州監査官）のデータに対する必要性。

F．エラー・コントロール

ＩＳＤの責任

1. システムはエラーの十分な識別手段をもたなければならない。

a．除去項目は全て，除去理由を示す意味とともに相応なエラー・リストに掲

載されなければならない。

b．共通のデータを使用しているシステムは，クロスチェックが容易となるようエラー・リスト上の当該データの識別に画一性をもたせるべきである。

c．除去理由を示す文字またはコードとともに，誤りのあるレコードの全体を別のエラー・データ・セットに書き込むことは，良いアイデアである。

2. 金銭的エラーの目録も必ず用意されなければならない（例，仮勘定）。これは，未修正のエラー追跡を可能とするからである。上述した1(c)のデータセットが利用できる。

a．ISDは，仮勘定リストのような未解決エラーのリストを作成し，備忘録として関係ユーザに提出すべきである。品目のエージングもまた良い手段といえる。

b．訂正は，トランザクションを意図通りマスタに照らして修正・処理することであり，ファイルや仮勘定・エラー・リストからトランザクションを除去することでもある。どちらの場合も，手直しした行為はトランザクション・レジスタかそれと同様のリストに現われ，その後点検のためユーザやユーザのコントロール・グループへ返送される。

3. エラーはユーザに戻され訂正されなければならない。この訂正においても，それだけの能力を有する高レベルのスタッフに戻すべきなのはいうまでもない。

4. 全ての欄の正確さを期すため，修正項目の再記帳（リエントリ）は必ずチェックする。以前に誤りのあった項目だけでなく，レコード全体の再チェックが必要である。

ユーザの責任

1. ユーザ側の管理では，つぎの事柄を確実にしなければならない。

a．仮勘定リストの点検と修正のスピードアップでエラー訂正の適時性を確保する。

b．エラー・リストの注視と過度のエラーをフォロー・アップすることによってエラー数を最低限に抑える。

c．修正手順は，最も迅速で，正確で，かつよくコントロールされた作業でなければならない。

2. エラー・リストの作成では，ユーザがつぎの項目について各エラーを修正するごとに，その旨表示が必要である。

a．訂正の日時

b．訂正の担当者

c．訂正されるトランザクションの取引ナンバまたはそれに代る識別記号

3. ユーザは，エラーの発生源をできる限り突きとめ，そのエラーの訂正に努めなければならない。

4. エラーは，ハードウェアまたはソフトウェアで発生したことが明らかである場合にのみ，ＩＳＤに照会される。

G．データ変更コントロール

ＩＳＤの責任

1. 製品ファイルやデータ・レコードに内容に影響を与えるどのような変更も，関係ユーザ部門の事前の文書による承認なしで，ＩＳＤによって行われるべきではない。

a．もし適切な時点で関係ユーザ部門の承認が得られないならば，その限りにおいて変更はあり得るが，その場合直ちに変更が行われた旨当該ユーザ部門に文書で通知されなければならない。

2. 製品データの変更は，意図した修正だけが実行されるよう制御されるべきである。

3. 製品データの変更は，変更されたデータ項目（できるならば，生じた変更自体も）を明確に表示するため，トランザクション・リストに反映させなければならない。このリスト作業の結果はユーザやユーザのコントロール・グループに送達され，変更の影響が当初の意図通りであるか否か検証される必要がある。

ユーザの責任

1. データ項目の変更は，そのシステム全体へのインパクトの見地から評価され

るべきである。もしユーザが，その変更の正当性と有害を及ぼさないという確信をもつことができたなら，ユーザは入力コントロールに従ってそれを承認することになる。

2. ユーザは，システムが作成したトランザクション・リストを点検し，望むべき変更のみがなされたかを確認すべきである。

H. ファイル・セキュリティ・コントロール

ＩＳＤの責任

1. 全てのテープ，ディスク・パックおよびデータセルは，容易に処理プログラムによりチェックできる適切な識別子（例，ファイル・ラベル）を備えなければならない。

2. 全てのファイル媒体は，レコード・カウントと批評欄（クリティカル・フィールド）(注4)を持ち，同時に処理プログラムにより対照されるトータルをもつようにすべきである。

3. 磁気媒体のファイルは全て，処理中の事故や災害で破壊された場合を考慮し，そのファイルの再生を可能とする十分なバックアップを備える必要がある。バックアップは，ファイル中のエラーの検知を可能とするだけの期間は確保されねばならない（例，ユーザ出力検査手順）。

4. 全ての製品データセットは，さかのぼって保護されるべきである。

ユーザの責任

1. ユーザが管理するファイル（例，パンチ・カードやある種の磁気テープ）には，つぎの事項に留意すべき必要性がある。

   a. つぎの項目の使用により，即座の識別を可能とするマークを添付すべきである。

      1) ラン・ナンバ

      2) ラン日時

      3) システム

      4) 場所の順序（例，４の１）

b．許可の無いアクセスや不注意による破壊から防護されるようファイルは蓄積されなければならない。

（注４）：本ガイドライン中で定義されている批評欄は，つぎの特長を有している。

- 総勘定元帳の収支残高による裏付け
- 処理あるいは処理結果の重視
- コントロールの実用性

Ⅱ．管理的コントロール

A．プログラム／システム・ドキュメンテーション

ＩＳＤの責任

1. アプリケーション・ラン・ブックやコンピュータ・センタ・ラン・ブックの標準は，ＩＳＤ標準および情報マニュアル（S&IM4.04－02および4.07－01）にそって最低限遵守されなければならない。
2. ＩＳＤは，ユーザ・マニュアルの作成に必要なレイアウト，フローチャート，機能表示の全てが時機を得て供給されるよう保証すべきである。
3. 全てのドキュメンテーションは，常に最新のものでなければならず，オリジナル・システムに起った変化の全てを反映したものでなければならない。

ユーザの責任

1. 当該システム向けの「ユーザ・マニュアル」の存在およびその完全さに，ユーザは絶えず関心を払う必要がある。これにはつぎの項目が含まれる。

   a．コントロールおよびインプットの機能的効果を含む作成用の入力レイアトと完全なインストラクション。

   b．出力レポートの定義および包括的な解釈の説明。

   c．エラーの修正ができるだけ速やかとなるようなエラー解釈・訂正手順。

   d．システム概要の表示に含まれるものはつぎの通り。

   1）その用途

2） システム機能の作動の仕方

3） ソース・ドキュメンテーション

4） その能力

5） 総合的なシステム運用の詳細表示（インタフェース目的，ファイル結果など）

B．プログラム変更コントロール

ＩＳＤの責任

1. 変更がなされる以前に，適切な許可がユーザから得られなければならない。
2. ＩＳＤは，変更されたプログラムの徹底的なテストを確実にし，そのプログラムが再び生産現場に投じられる以前に，テスト結果についてのユーザの正式な承認が得られるようにする。
3. プログラムの変更により影響を受けたドキュメンテーションの全て（システム，ユーザ，プログラム）は，その変更を反映するよう改変されなければならない。
4. 会計手法の全ての変更は文書化され，ユーザと会計部門の双方より正式の承認をうける必要がある。

ユーザの責任

1. ユーザの要求するあらゆる変更は，責任あるユーザからの文書による許可要請に基づかなければならない。
2. プログラム変更にまつわる品質管理の一方法として，ユーザは既存システムに重大な変化が発生したか否かをテストすることもあり得る。
3. ＩＳＤのプログラム変更テストの結果は，生産現場に導入される以前に，他の影響を受けるシステムのユーザだけでなく，中心システムのユーザからも正式の承認をとりつける必要がある。
4. 全てのユーザ・マニュアルは，プログラム変更によりもたらされた変化を反映するよう更新されなければならない。

Ⅲ．組織的コントロール

A．責任の分担

ＩＳＤの責任

1. 全てのコンピュータ・システムにおいてＩＳＤの介入は，それをランし展開させる機能に分離されなければならない。

   a．コンピュータ・システムの開発者は，それをランさせる者と同一人物であってはならない。アプリケーションやオペレーションも機能ごとに分割されるべきである。

2. ＩＳＤは，当該システムへのユーザの要求にそって，システムの運用スケジュールに責任をもつものとする。

ユーザの責任

1. 全てのコンピュータ・システムにおけるユーザの介入は，エントリ・データを提供する機能，それに許可を与える機能，戻り出力の受領・点検を担当する機能等に分離されなければならない。

   a．入力データの作成者は，入力の許可者と同一であってはならない。

   b．入力データに許可を与えた者は，そのデータの作成者と重複してはならない。

   c．システム出力の受領・検査を行う者は，入力の作成者と同一人物であってはならない。

2. 対象システムをいつランさせるかを決定するのはユーザである。

B．マネジメント・トレイル

ＩＳＤの責任

1. 直接間接を問わず，企業の会計簿に影響を与える全てのシステムにとって，つぎの要件が満たされなければならない。

   a．記帳のサポート ― システムは，それが生成した合計の記帳のために詳細なサポートを作成するか，要請に応じて作成する能力をもたなければならない。

b．収支のサポート — システムは，企業の帳簿で資産と負債の帳尻をサポートするため，ハードコピーの詳細な試算表を作成するか，要請に応じて作成する能力をもたなければならない。

2. 監査証跡は，トランザクションの最初から最後までの追跡を可能とするため，全てのシステムに組み込まれる必要がある。その逆方向あるいは往復型の追跡もできれば用意しだい。

a．監査証跡は，最初のソースからコンピュータ環境における記帳，そして処理結果のプリントアウトおよび帳簿への最終的な転記までのトランザクション追跡能力をもつ。

b．反対に，証跡は，マスタ・レコードの更新前の状態を再構成することも可能である。

1) 現状のプリントアウト，マスタ・レコード，トランザクション・レジスタ等に「最終取引期日／最終取引形態」を記入することにより，この方法が実施される。

3. トランザクション処理後，十分なサポーティング・ドキュメンテーションが適切な期間利用できるようにすべきである。

4. ＥＤＰシステムにおけるデータの集約は，監査証跡を妨害したり，その価値を減じるものではない。

5. ネットワークにおけるような直接入力は，監査証跡の不可欠要素としてのソース・ドキュメントや認可要件の必要性を軽視しはしない。

6. マスタ・ファイルの収支残高は，常にその構成部分と関連づけられなければならない。

ユーザの責任

1. トランザクション処理後，十分なサポーティング・ドキュメンテーションが適切な期間利用できるようにすべきである。

2. ソース・ドキュメントは，以後の検索が容易となるようファイルされなければならない。

3. 出力ドキュメントは，以後の検索が容易となるようファイルされなければならない。

付録A　様々なコントロールが証明すべき事柄の概要

入力コントロール

- データは合法的である。
- データは正確でかつ完全である。
- データは正確かつ完全に転送されている。

処理コントロール

- 許可されたファイルの利用。
- ファイルは正しい。
- データはプログラムとシステム間で正確かつ完全に転送されている。
- 出力は入力に正確かつ完全に基づいたものである。

出力コントロール

- 出力は入力＋（プラス）トランザクション，または入力－（マイナス）トランザクションに等しい。
- 出力は完全で正確である。
- 出力は均整がとれている。
- 出力はその理解が容易なように設計されている。
- 出力は必要である。
- 出力は許可を与えられた受け取り手に渡っている。

直接的更新手法を使用したシステムのコントロール

- 許可されたユーザだけがアクセスを許されている。
- 無許可の更新は最大限に困難である。
- 無許可の更新は手順の均衡で出来る限りキャッチされている。

データ保存

- 保存は全ての要件（法律，ＩＲＳ，システム・バックアップなど）を満たし

ている。

エラー・コントロール

- エラーは完全かつ正確に発見され訂正されている。
- エラーは速かに修正される。
- エラーの量は過大ではない。

データ変更コントロール

- 変更は許可をうけたものである。
- 変更は完全である。

ファイル・セキュリティ

- ファイルは適切に識別されている。
- ファイルは十分保護されている。
- ファイルは十分なバックアップをもっている。
- 意図的でかつ許可をうけたアクセスだけが許されている。

ドキュメンテーション

- (最低の要件である)標準および情報マニュアルの要件が満たされている。
- ドキュメンテーションは最新のものである。
- ユーザ・マニュアルは完全でかつ正確である。

プログラム変更コントロール

- 変更は許可されたものである。
- 変更は完全である。
- 変更のドキュメント化は十分である。
- テストは完全であり，関係者の満足を得ている。
- コンバージョンのインパクトは非常に少ない。
- ユーザは事前に準備できている。
- ドキュメンテーションは更新されている。

責任の分担

- コントロールが維持できるほど完全である。

マネジメント・トレイル

- 証跡は完全でかつ正確である。
- 証跡は双方向型である。

付　録　B

入力コントロールの定義

入力コントロール	定　　義	例
コントロール・トータル	ファイル・レコードの特定欄に記載された価格の金額および件数の合計。 ファイルの管理に用いられる。	ある時点までの給与支払ファイルに記入された通年給与合計は 784,964.5ドル
バッチ平衡	全項目が処理済みか否かを確認するため，確定している照査合計と実際に処理された項目を比較すること。	入　力　　コントロール 20　レコード　20 112925638　保険証券番号ハッシュ　112925638 2565.99　保険料合計　2565.99
バッチ・コントロール・ログ	バッチまたはトランザクションの照査数値および関係詳細を内容とするログ	7／22／76 ― バッチ＃41-100 レコード ― 保険料合計 921,475.37ドル 保険証券ハッシュ・トータル 894,371,711
バッチ・コントロール・トータル	特定の組合せのトランザクションに適用されるコントロール，ハッシュまたはレコード・カウントの合計。トランザクションはこのトータルと均衡している。	２０レコードの最初のバッチは，保険証券のハッシュ合計が112,925,638で，保険料合計は2,747ドルであった。
バッチ番号チェック	全項目が処理中のバッチに属するものであることを確認するため行う個々のバッチ項目上のバッチ番号とコントロール・バッチ番号の比較対照。	
チェック・ディジット	欄の内容を検査するため使用される数字。欄内では数学的な機能の数字であり，特殊数字として添加される。その値は，欄の有効性をチェックするため算定・比較し得る。	欄　276924 乗因数　21212 4+7+12+9+4＝36 -40 チェック・ディジット　4
完全性チェック	データを事実上含んでいるか，データを含まねばならない欄を検証するチェック	チェックは，受取人または金額の欄が空白の場合，プリントされてはならない。

入力コントロール	定　　義	例
一貫性テスト	特定欄の内容が他の関連欄の内容と一致しているかを確認する検査。 一貫性テストは，また同じデータを使用している別のプログラムが共通の形でそのデータを扱っているかを確認するのに用いる。	支払済みの保険証券は，保険料支払日に記入があってはならない。プログラムAの月間保険料がプログラムBに移された途端，年間保険料として扱われてはならない。
データ予測	ある時点またはある条件における特定のトランザクションやデータ項目を予測すること。	給与支払システムは，どの給料未支払従業員も週40時間と計算していると予測する。
フォーマット・チェック	特定欄のデータのフォーマットが適切かどうかをチェックすること（数字あるいはアルファベット）。	一連の文字72P×192は，正しい保険証券番号ではない。
ハッシュ・トータル	非金銭欄の数値量の合計でファイルまたはバッチのコントロールに用いられる（金額照査合計と対応）。	ファイル・レコードの保険証券番号のハッシュ合計は，7,829,771,592,346である。
見出しラベル	ソース，アプリケーション，日付け，あるいはその他の識別指標に対するファイルまたはバッチの内部識別物。	
入出力コントロール・グループ	入力，そのバッチ，コントロールの完全性，出力の完全性，出力の配布を確実にする責任を負う個人またはグループ。これは明確に入力準備と分離されねばならない。	
キーストローク検証	パンチカードへの最初の入力が正確か否かをチェックするため，データを再びキーパンチでエントリすること。偏差は機械的にキーパンチャに通知される。	
限界テスト	指定された上下限値をもとに，特定の数値欄が適合しているか否かチェックするテスト。	保険証券の貸付利率が1ドル以下なら記載する必要がない。
ライン・コントロール・トータル	印刷された出力の行数のトータル数。	5月の保険証券貸付ジャーナルは47,000件のエントリを含んでいた。
機械読取可能ドキュメント	磁気的にドキュメント上にコード化されているデータ。このデータはコンピュータ周辺機器で直接読み取れる。	小切手末尾の口座番号は磁気的にコード化されている。
オーバフロー・チェック	欄の容量をもとに，その中のデータのサイズをチェックすること。	10×499.50の積は5桁欄には入りきれない。

入力コントロール	定　　義	例
レンジ・テスト	一定の上下限数値をもとにある数値欄をチェックすること。	5％の保険証券貸付利率は，証書番号1350470から4549999の間にのみ適用される。
合理性テスト	レコードやトランザクションの他の欄に含まれているデータと比較してデータ欄をチェックすること。	額面1万ドルの保険証券は，月間保険料7,995.97ドルとはならない。
レコード・カウント	ファイルまたはバッチ中の個々のレコード数の算定。	給与支払ファイルは7,043件のレコードを有している。
インプット正当性チェック・ラン	入力が処理にまわされる前に，その有効性をチェックするためシステム内に含まれているプログラム。一般には多数の有効性チェックを組合せたものが多い。	これらのプログラムは入力編集プログラムと呼ばれるのが普通である。
シーケンス・チェック	処理されるレコードまたはトランザクションの識別子またはキー欄内の数値順序をチェックすること。	保険証券番号4 216 961は，順序として5 096 712に先行し，4 216 942の後にしなければならない。
通し番号	ドキュメントやバッチは，そのコントロールを容易にするため，順序立てて番号を与えられるべきである。	小切手に記載されたチェック・ナンバ
視覚確認	ドキュメントの完全性や合理性を視覚で点検すること。	
視覚確認－ＣＲＴ	データがＣＲＴ端末から入力される時，そのデータはすぐにその端末のディスプレイ上に現われ，送り手自身が目でチェックできる仕組みとなっている。データは送り手がこの検査を終えた後はじめてシステムにより受け付けられる。	
後書きラベル	ファイル上のレコードのカウント合計とコントロール・トータルを含むファイル・レコードで，レコード処理中の累積値と比較される。	
単一構造テスト	単一構造を必要とするか，正にそういう構造をもっている欄（または欄のセット）を確認するテスト。	日付け欄は，年（２文字），月（２文字），日（２文字）から構成されている。
正当性テスト	フォーマット，数値，コード等の要件をデータ欄が満たしているかをチェックすること。数値は表や算定ルーチンを使っても検査できる。	現在の日付け項目は6桁であり，7621は是認できるが760201は認められない。

(注) この表の主要情報提供源は，Tauche, Ross & Co. の Computer Control and Audit である。

Bibliography

1. Security, Accuracy, and Privacy in Computer Systems
   by James Martin of the IBM Systems Research Institute
   1973

2. Security for Computer Systems
   by The National Computing Center, Ltd.
   1973

3. Security Standards for Data Processing
   Wooldridge, Corder, and Johnson
   1973

4. Computer Control and Audit
   Touche, Ross & Co.
   1976

5. Management Controls in Data Processing
   IBM Manual

6. Basic System Controls
   by Aetna's Data Processing Educational Program (ADPEP)

7. "Auditing Aspects of Data Processing"
   Data Management, July 1972, page 17

8. "Auditing Control and Systems Design"
   by Eoster Brown; presented in the Journal of System Management, April 1975

9. Data Control Guidelines
   by J.R. Sharralt, National Computing Center, Ltd. as reviewed by the Automation Training Center in EDPACS, October 1975, page 12

10. Systems Analyst Training Program
    by DELTAK

11. "Why Document"
    Data Management, January 1975, page 6

12. Computer Control Guidelines
    The Canadian Institute of Chartered Accountants
    1972

13. Computer Audit Guidelines
The Canadian Institute of Chartered Accountants, 1975

14. "EDP Security Control"
The Internal Auditor, July/August 1974, page 16

15. "EDP Controls to Check Fraud"
Management Accounting, October 1974, page 43

16. "The EDP Technician, The Accountant, and Internal Control"
Management Accounting, September 1975, page 38

17. The Practice of Modern Internal Auditing
by Lawrence Sawyer, The Institute of Internal Auditors, 1973

18. The Handbook for Auditors
James Cashin, editor-in-chief, 1971

19. The Effects of EDP on the Auditors Study of Evaluation of Internal Control
Statement on Auditing Standards #3, by the Auditing Standards Committee, AICPA, December 1974

20. "An Audit Perspective of Operating System Security"
The Journal of Accountancy, September 1975, page 97

昭和57年8月発行

発行所　財団法人　日本情報処理開発協会
東京都港区芝公園3丁目5番8号
機械振興会館内
TEL（434）8211（代表）

印刷所　三協印刷株式会社
東京都渋谷区渋谷3丁目11番11号
TEL（407）7316